

Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle Identity Management
(Oracle Fusion Applications Edition)

11g Release 5 (11.1.5)

E21032-15

November 2012

Documentation for system administrators that describes how to install and configure Oracle Identity Management components in an enterprise deployment for Oracle Fusion Applications.

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition), 11g Release 5 (11.1.5)

E21032-15

Copyright © 2004, 2012, Oracle and/or its affiliates. All rights reserved.

Primary Authors: Ellen Desmond (Writer), Janga Aliminati (Architect), Michael Rhys (Contributing Engineer)

Contributors: Vasuki Ashok, Pradeep Bhat, Bruce Jiang, Louise Luo, Xiao Lin, Jingjing Wei

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Preface	xix
Audience	xix
Documentation Accessibility	xix
Related Documents	xix
Conventions	xx
What's New in This Guide	xxi
New and Changed Features for 11g Release 5 (11.1.5)	xxi
1 Enterprise Deployment Overview	
1.1 About the Enterprise Deployment Guide	1-1
1.2 Enterprise Deployment Terminology	1-2
1.3 Benefits of Oracle Recommendations	1-5
1.3.1 Built-in Security	1-5
1.3.2 High Availability	1-6
2 Introduction to the Enterprise Deployment Reference Topologies	
2.1 Overview of Enterprise Deployment Reference Topologies	2-1
2.1.1 Reference Topologies Documented in the Guide	2-1
2.1.1.1 Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications	2-2
2.1.1.2 Split Domain Topology for Oracle Fusion Applications	2-3
2.1.1.3 Oracle Identity Federation 11g for Fusion Applications	2-4
2.1.2 About the Directory Tier	2-5
2.1.2.1 High Availability Provisions	2-7
2.1.3 About the Application Tier	2-7
2.1.3.1 Architecture Notes	2-8
2.1.3.2 High Availability Provisions	2-9
2.1.3.3 Security Provisions	2-9
2.1.4 About the Web Tier	2-9
2.1.4.1 Architecture Notes	2-9
2.1.4.2 High Availability Provisions	2-10
2.1.4.3 Security Provisions	2-10
2.2 Hardware Requirements for an Enterprise Deployment	2-10
2.3 Identifying the Software Components to Install	2-11

2.4	Road Map for the Reference Topology Installation and Configuration	2-11
2.4.1	Flow Chart of the Oracle Identity Management Enterprise Deployment Process for Oracle Fusion Applications	2-12
2.4.2	Steps in the Oracle Identity Management Enterprise Deployment Process	2-14

3 Preparing the Network for an Enterprise Deployment

3.1	Overview of Preparing the Network for an Enterprise Deployment	3-1
3.2	About Virtual Server Names Used by the Topologies	3-1
3.2.1	oididstore.mycompany.com	3-2
3.2.2	polycystore.mycompany.com	3-2
3.2.3	idstore.mycompany.com	3-3
3.2.4	admin.mycompany.com	3-3
3.2.5	oimadmin.mycompany.com	3-4
3.2.6	idminternal.mycompany.com	3-4
3.2.7	sso.mycompany.com	3-4
3.3	Configuring the Load Balancers	3-4
3.3.1	Load Balancer Requirements	3-5
3.3.2	Load Balancer Configuration Procedures	3-6
3.4	Load Balancer Configuration	3-6
3.5	About IP Addresses and Virtual IP Addresses	3-8
3.6	About Firewalls and Ports	3-11
3.7	Managing Oracle Access Manager Communication Protocol	3-14
3.7.1	Oracle Access Manager Protocols	3-14
3.7.2	Overview of Integration Requests	3-14
3.7.3	Overview of User Request	3-14
3.8	About WebLogic Domains	3-15

4 Preparing the File System for an Enterprise Deployment

4.1	Overview of Preparing the File System for Enterprise Deployment	4-1
4.2	Terminology for Directories and Directory Variables	4-1
4.3	ASERVER_HOME and MSERVER_HOME	4-2
4.4	About Recommended Locations for the Different Directories	4-3
4.4.1	Local Storage	4-4
4.4.2	Shared Storage	4-4
4.4.3	Redundant Binary Installations	4-5
4.4.4	Directory Structure	4-6
4.5	Configuring Shared Storage	4-8

5 Preparing the Database for an Enterprise Deployment

5.1	Overview of Preparing the Databases for an Identity Management Enterprise Deployment	5-1
5.2	Verifying the Database Requirements for an Enterprise Deployment	5-1
5.2.1	Databases Required	5-2
5.2.2	Database Host Requirements	5-2
5.2.3	Database Versions Supported	5-3
5.2.4	Patching the Oracle Database	5-3

5.2.4.1	Patch Requirements for Oracle Database 11g (11.1.0.7)	5-3
5.2.4.2	Patch Requirements for Oracle Database 11g (11.2.0.2.0)	5-3
5.2.5	About Initialization Parameters	5-4
5.3	Installing the Database for an Enterprise Deployment	5-5
5.4	Creating Database Services	5-6
5.4.1	Creating Database Services for 10.x and 11.1.x Databases	5-6
5.4.2	Creating Database Services for 11.2.x Databases	5-7
5.4.3	Database Tuning	5-8
5.5	Loading the Identity Management Schemas in the Oracle RAC Database by Using RCU	5-9
5.6	Backing up the Database	5-10

6 Installing the Software for an Enterprise Deployment

6.1	Overview of the Software Installation Process	6-1
6.1.1	Obtaining the Software	6-1
6.1.2	Software to Install	6-2
6.2	Installing Oracle HTTP Server	6-3
6.2.1	Verifying Prerequisites	6-3
6.2.1.1	Check oraInst.loc	6-4
6.2.2	Running the Installer	6-4
6.2.3	Backing Up the Installation	6-5
6.3	Installing Oracle Fusion Middleware	6-5
6.3.1	Installing Oracle Fusion Middleware Components	6-5
6.3.2	Installing Oracle Fusion Middleware Home	6-6
6.3.3	Installing Oracle WebLogic Server and Creating the Fusion Middleware Home	6-7
6.3.4	Installing Oracle Identity Management	6-8
6.3.5	Installing the Oracle SOA Suite	6-9
6.3.6	Installing Oracle Identity and Access Management	6-11
6.3.7	Applying Patches and Workarounds	6-12
6.3.7.1	Patches for Fusion Middleware	6-12
6.3.7.2	Provisioning the OIM Login Modules Under the WebLogic Server Library Directory	6-12
6.3.7.3	Creating the wfullclient.jar File	6-13
6.3.8	Backing Up the Installation	6-13

7 Configuring the Web Tier for an Enterprise Deployment

7.1	Overview of Configuring the Web Tier	7-1
7.2	Prerequisites for Configuring the Web Tier	7-1
7.3	Running the Configuration Wizard to Configure the HTTP Server	7-2
7.4	Validating the Configuration	7-3
7.5	Configuring Virtual Hosts and Server Owner	7-3
7.5.1	Configuring Virtual Hosts	7-3
7.5.2	Configuring Oracle HTTP Server to Run as Software Owner	7-4
7.5.3	Update Oracle HTTP Server Runtime Parameters	7-5
7.5.4	Restarting the Oracle HTTP Servers	7-5
7.5.5	Validating the Configuration	7-5
7.6	Backing up the Web Tier Configuration	7-6

8 Creating Domains for an Enterprise Deployment

8.1	Overview of Creating a Domain	8-1
8.2	Choosing Single Domain or Split Domain	8-2
8.3	About Console URLs and Domains	8-2
8.4	Synchronize System Clocks	8-3
8.5	Enabling Virtual IP Addresses for Use by the Domain	8-3
8.5.1	Enabling Virtual IP Addresses for Administration Servers	8-3
8.6	Running the Configuration Wizard to Create a Domain with Oracle Access Manager, Oracle SOA Suite, and Oracle Identity Manager	8-4
8.7	Post-Configuration and Verification Tasks	8-13
8.7.1	Creating boot.properties for the WebLogic Administration Server on IDMHOST1	8-13
8.7.2	Creating boot.properties for the WebLogic Administration Server on OIMHOST1	8-14
8.7.3	Starting Node Manager	8-14
8.7.4	Updating the Node Manager Credentials	8-14
8.7.5	Validating the WebLogic Administration Server	8-16
8.7.6	Removing IDM Domain Agent on IDMHOST1	8-16
8.7.7	Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server	8-17
8.7.8	Propagate Changes to Remote Servers	8-17
8.7.9	Copy SOA Composites to Managed Server Directory	8-18
8.7.10	Start Node Manager on Remote Hosts	8-18
8.7.11	Disabling Host Name Verification for the Oracle WebLogic Administration Server	8-19
8.7.12	Stopping and Starting the WebLogic Administration Server	8-19
8.8	Configuring Oracle HTTP Server for the WebLogic Domain	8-20
8.8.1	Configuring Oracle HTTP Server for the WebLogic Administration Server	8-20
8.8.2	Configuring Oracle HTTP Server for the Oracle Identity Manager Domain	8-21
8.8.3	Restart Oracle HTTP Server	8-22
8.8.4	Registering Oracle HTTP Server with WebLogic Server	8-22
8.8.5	Setting the Front End URL for the Administration Console	8-22
8.8.6	Enabling WebLogic Plug-in	8-23
8.8.7	Validating Access to Domains	8-24
8.9	Manually Failing Over the WebLogic Administration Server	8-24
8.9.1	Failing over the Administration Server to IDMHOST2	8-24
8.9.2	Starting the Administration Server on IDMHOST2	8-26
8.9.3	Validating Access to IDMHOST2 Through Oracle HTTP Server	8-27
8.9.4	Failing the Administration Server Back to IDMHOST1	8-27
8.10	Backing Up the WebLogic Domain	8-28

9 Extending the Domain to Include Oracle Internet Directory

9.1	Overview of Extending the Domain to Include Oracle Internet Directory	9-1
9.2	Using Oracle Internet Directory in an Enterprise Deployment	9-1
9.3	Prerequisites for Configuring Oracle Identity Directory Instances	9-2
9.4	Configuring the Oracle Internet Directory Instances	9-2
9.4.1	Configuring the First Oracle Internet Directory Instance	9-2
9.4.2	Configuring an Additional Oracle Internet Directory Instance	9-5
9.5	Post-Configuration Steps	9-7

9.5.1	Registering Oracle Internet Directory with the WebLogic Server Domain (IDMDomain)	9-8
9.5.2	Generating a Certificate to be Used by the Identity Management Domain	9-9
9.5.2.1	Prerequisites	9-10
9.5.2.2	Generating the Certificate	9-10
9.5.3	Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections	9-12
9.5.3.1	Prerequisites	9-12
9.5.3.2	Configuring Oracle Internet Directory for SSL	9-12
9.5.4	Validating SSL Manually	9-14
9.5.5	Considering Oracle Internet Directory Password Policies	9-15
9.6	Validating the Oracle Internet Directory Instances	9-15
9.7	Tuning Oracle Internet Directory	9-16
9.8	Backing up the Oracle Internet Directory Configuration	9-16

10 Extending the Domain to Include ODSM

10.1	Overview of Extending the Domain to Include ODSM	10-1
10.2	Prerequisites	10-1
10.3	Extending the Oracle WebLogic Domain IDMDomain	10-2
10.4	Expanding the ODSM Cluster	10-3
10.5	Provisioning the Managed Servers in the Managed Server Directory	10-5
10.6	Configuring ODSM to work with the Oracle Web Tier	10-6
10.6.1	Prerequisites	10-7
10.6.2	Configuring Oracle HTTP Servers to Access the ODSM Console	10-7
10.7	Validating the Application Tier Configuration	10-7
10.7.1	Validating Browser Connection to ODSM Site	10-7
10.7.2	Validating ODSM Connections to Oracle Internet Directory	10-8
10.8	Backing Up the Application Tier Configuration	10-8

11 Preparing Identity and Policy Stores

11.1	Overview of Preparing Identity and Policy Stores	11-1
11.2	Backing up the LDAP Directories	11-1
11.3	Prerequisites	11-1
11.4	Preparing the OPSS Policy Store	11-2
11.4.1	Creating Policy Store Users and the Policy Container	11-2
11.4.2	Reassociating the Policy and Credential Store	11-4
11.4.3	Associate OIMDomain with Policy and Credential Store	11-5
11.5	Preparing the Identity Store	11-6
11.5.1	Creating the Configuration File	11-7
11.5.2	Preparing a Directory for Oracle Access Manager and Oracle Identity Manager	11-8
11.5.2.1	Configuring Oracle Internet Directory for Use with Oracle Access Manager and Oracle Identity Manager	11-8
11.5.2.2	Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Manager	11-10
11.5.3	Creating Users and Groups	11-11
11.5.4	Creating Access Control Lists in Non-Oracle Internet Directory Directories	11-12

12 Extending the Domain to Include Oracle Virtual Directory

12.1	Overview of Extending the Domain to Include Oracle Virtual Directory	12-1
12.2	Prerequisites for Configuring Oracle Virtual Directory Instances	12-1
12.3	Configuring the Oracle Virtual Directory Instances	12-2
12.3.1	Configuring the First Oracle Virtual Directory Instance	12-2
12.3.2	Configuring an Additional Oracle Virtual Directory	12-4
12.4	Post-Configuration Steps	12-5
12.4.1	Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain (IDMDomain)	12-6
12.4.2	Configuring Oracle Virtual Directory to Accept Server Authentication Only Mode SSL Connections	12-7
12.4.2.1	Prerequisites	12-7
12.4.2.2	Configuring Oracle Virtual Directory for SSL	12-8
12.5	Disable Oracle Virtual Directory LDAP Listeners NIO	12-9
12.6	Validating the Oracle Virtual Directory Instances	12-10
12.7	Creating ODSM Connections to Oracle Virtual Directory	12-11
12.8	Creating Adapters in Oracle Virtual Directory	12-11
12.8.1	Ensuring the Change Log Generation is Enabled in Oracle Internet Directory	12-11
12.8.2	Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory	12-12
12.8.3	Validating the Oracle Virtual Directory Adapters	12-14
12.9	Backing Up the Oracle Virtual Directory Configuration	12-15

13 Configuring Oracle Access Manager 11g

13.1	Overview of Configuring Oracle Access Manager	13-1
13.2	About Domain URLs	13-2
13.3	Using Different Directory Configurations	13-2
13.4	Prerequisites	13-2
13.5	Starting Oracle Access Manager Managed Servers	13-3
13.6	Configuring Oracle Access Manager to work with the Oracle Web Tier	13-3
13.6.1	Prerequisites	13-3
13.6.2	Configuring Oracle HTTP Servers to Display Login Page	13-3
13.6.3	Configuring Oracle HTTP Servers to Access Oracle Access Manager Console	13-4
13.7	Configuring Oracle Access Manager	13-5
13.7.1	Setting a Global Passphrase	13-5
13.7.2	Configuring Oracle Access Manager by Using the IDM Automation Tool	13-5
13.7.3	Validating the Configuration	13-9
13.7.4	Updating Newly-Created Agent	13-9
13.7.5	Updating Existing WebGate Agents	13-10
13.7.6	Perform Bug 13824816 Workaround	13-10
13.7.7	Configuring Oracle Access Manager for Multidirectory Support	13-11
13.8	Adding the oamadmin Account to Access System Administrators	13-11
13.9	Create Oracle Access Manager Policies for WebGate 11g	13-12
13.10	Creating Oracle Access Manager Key Store	13-12
13.10.1	Creating an Empty Trust Store File Named oamclient-truststore.jks	13-12
13.10.2	Importing the CA Certificate into the Trust Store	13-13

13.10.3	Setting up Keystore with the SSL Certificate and Private Key File of the Access Client .	13-14
13.11	Updating Oracle Access Manager System Parameters	13-15
13.12	Backing Up the Application Tier Configuration	13-16

14 Configuring Oracle Identity Manager

14.1	Overview of Configuring Oracle Identity Manager	14-2
14.2	About Domain URLs	14-2
14.3	Prerequisites	14-2
14.4	About the Split Oracle Identity Manager Domain	14-3
14.5	Synchronize System Clocks	14-3
14.6	Configuring Oracle Identity Manager	14-3
14.7	Configuring Oracle Coherence for Deploying Composites	14-6
14.7.1	Enabling Communication for Deployment Using Unicast Communication	14-6
14.7.2	Specifying the Host Name Used by Oracle Coherence	14-6
14.8	Post-Installation Steps on OIMHOST1	14-8
14.8.1	Starting the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1	14-8
14.8.2	Validating Oracle Identity Manager Instance on OIMHOST1	14-9
14.9	Post-Installation Steps on OIMHOST2	14-9
14.9.1	Starting Node Manager on OIMHOST2	14-9
14.9.2	Starting the WLS_OIM2 and WLS_SOA2 Managed Servers on OIMHOST2	14-9
14.9.3	Validating Oracle Identity Manager Instance on OIMHOST2	14-10
14.10	Modifying the Oracle Identity Manager Properties to Support Active Directory	14-10
14.11	Configuring Oracle Identity Manager to Reconcile from ID Store	14-10
14.12	Configuring Oracle Identity Manager to Work with the Oracle Web Tier	14-11
14.12.1	Prerequisites	14-12
14.12.2	Configuring Oracle HTTP Servers to Front End the Oracle Identity Manager and SOA Managed Servers	14-12
14.12.3	Changing Host Assertion in WebLogic	14-15
14.12.4	Validating Oracle Identity Manager Instance from the WebTier	14-16
14.12.5	Validating SOA Instance from the WebTier	14-16
14.13	Configuring a Default Persistence Store for Transaction Recovery	14-16
14.14	Configuring an IT Resource Instance for Email	14-17
14.15	Enabling Oracle Identity Manager to Connect to SOA Using the Administrative Users Provisioned in LDAP	14-18
14.16	Updating the Username Generation Policy for Active Directory	14-19
14.17	Tuning Oracle Platform Security	14-20
14.18	Provisioning Users to the Enterprise Identity Store in a Multidirectory Scenario	14-21
14.18.1	Creating and Importing New Rules	14-21
14.18.2	Updating IT Resource for Oracle Identity Manager Integration	14-22
14.18.3	Updating the Incremental Reconciliation Changelog Number	14-22
14.19	Excluding Users from Oracle Identity Manager Reconciliation	14-23
14.19.1	Adding the orclAppIDUser Object Class to the User by Using ODSM	14-24
14.19.2	Closing Failed Reconciliation Events by Using the OIM Console	14-24
14.20	Backing Up the Application Tier Configuration	14-24

15 Extending the Domain to Include Oracle Identity Federation

15.1	Overview of Extending the Domain to Include Oracle Identity Federation	15-1
15.2	Prerequisites	15-2
15.3	Configuring Oracle Identity Federation on IDMHOST1	15-2
15.4	Run Upgrade Script	15-6
15.5	Configuring Oracle Identity Federation on IDMHOST2	15-7
15.6	Provisioning the Managed Servers on the Local Disk	15-8
15.7	Validating Oracle Identity Federation	15-10
15.8	Configure the Enterprise Manager Agents	15-10
15.9	Enabling Oracle Identity Federation Integration with LDAP Servers	15-10
15.10	Configuring Oracle Identity Federation to work with the Oracle Web Tier	15-12
15.10.1	Prerequisites	15-12
15.10.2	Making Oracle Identity Federation aware of the Load Balancer	15-12
15.10.3	Configuring Oracle HTTP Servers To Front End the Oracle Identity Federation Managed Servers	15-13
15.11	Validating Oracle Identity Federation	15-13
15.12	Backing Up the Application Tier Configuration	15-13

16 Setting Up Node Manager for an Enterprise Deployment

16.1	Overview of the Node Manager	16-1
16.2	Changing the Location of the Node Manager Log	16-2
16.3	Enabling Host Name Verification Certificates for Node Manager	16-2
16.3.1	Generating Self-Signed Certificates Using the utils.CertGen Utility	16-3
16.3.2	Creating an Identity Keystore Using the utils.ImportPrivateKey Utility	16-4
16.3.3	Creating a Trust Keystore Using the Keytool Utility	16-5
16.3.4	Configuring Node Manager to Use the Custom Keystores	16-6
16.3.5	Using a Common or Shared Storage Installation	16-6
16.3.6	Configuring Managed WebLogic Servers to Use the Custom Keystores	16-6
16.3.7	Changing the Host Name Verification Setting for the Managed Servers	16-8
16.4	Starting Node Manager	16-8

17 Configuring Server Migration for an Enterprise Deployment

17.1	Overview of Server Migration for an Enterprise Deployment	17-1
17.2	Setting Up a User and Tablespace for the Server Migration Leasing Table	17-1
17.3	Creating a Multi Data Source Using the Oracle WebLogic Administration Console	17-2
17.4	Editing Node Manager's Properties File	17-4
17.5	Setting Environment and Superuser Privileges for the wlsifconfig.sh Script	17-5
17.6	Configuring Server Migration Targets	17-6
17.7	Testing the Server Migration	17-7

18 Integrating Oracle Identity Management Components for an Enterprise Deployment

18.1	Overview of Integrating Oracle Identity Management Components	18-1
18.2	Integrating Oracle Identity Manager and Oracle Access Manager 11g	18-1
18.2.1	Prerequisites	18-2
18.2.2	Copying OAM Keystore Files to OIMHOST1 and OIMHOST2	18-2

18.2.3	About the Split Oracle Identity Manager Domain	18-2
18.2.4	Updating Existing LDAP Users with Required Object Classes	18-2
18.2.5	Integrating Oracle Access Manager 11g with Oracle Identity Manager 11g	18-6
18.2.6	Managing the Password of the xelsysadm User	18-12
18.2.7	Validating Integration	18-12
18.3	Preparing the Environment for Fusion Applications Provisioning	18-13
18.3.1	About Input to the Fusion Applications Provisioning Tool	18-13
18.3.2	Creating a Client Keystore	18-13
18.4	Integrating Oracle Identity Federation with Oracle Access Manager 11g	18-15
18.4.1	Prerequisites	18-15
18.4.2	Integrating Oracle Identity Federation with Oracle Access Manager in SP Mode ..	18-15
18.4.2.1	Configuring the Oracle Access Manager 11g SP Engine	18-15
18.4.2.2	Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager	18-18
18.4.3	Switching from Local Authentication to Federation SSO	18-18
18.5	Backing Up the Identity Management Configuration	18-19

19 Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment

19.1	Overview of Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment	19-1
19.2	Prerequisites	19-2
19.3	Create WebLogic Security Providers	19-2
19.3.1	Creating Oracle Directory Authenticator	19-2
19.3.2	Creating Oracle Access Manager Identity Asserter	19-4
19.4	Assigning WLSAdmins Group to WebLogic Administration Groups	19-5
19.5	Register EM with OPSS Security Provider	19-6
19.6	Updating the boot.properties File	19-6
19.6.1	Update the Administration Server on IDMHOST1	19-6
19.6.2	Update the Administration Server on OIMHOST1	19-7
19.6.3	Restarting the Servers	19-7
19.7	Installing and Configuring WebGate 11g	19-7
19.7.1	Prerequisites	19-8
19.7.2	Making Special gcc Libraries Available	19-8
19.7.3	Installing Oracle WebGate on WEBHOST1 and WEBHOST2	19-8
19.8	Validating WebGate and the Oracle Access Manager Single Sign-On Setup	19-9

20 Managing the Topology for an Enterprise Deployment

20.1	Starting and Stopping Oracle Identity Management Components	20-1
20.1.1	Startup Order	20-2
20.1.2	Starting and Stopping Oracle Virtual Directory	20-2
20.1.2.1	Starting Oracle Virtual Directory	20-2
20.1.2.2	Stopping Oracle Virtual Directory	20-2
20.1.3	Starting and Stopping Oracle Internet Directory	20-2
20.1.3.1	Starting Oracle Internet Directory	20-2
20.1.3.2	Stopping Oracle Internet Directory	20-3

20.1.4	Starting, Stopping, and Restarting Oracle HTTP Server	20-3
20.1.4.1	Starting Oracle HTTP Server	20-3
20.1.4.2	Stopping Oracle HTTP Server	20-3
20.1.4.3	Restarting Oracle HTTP Server	20-3
20.1.5	Starting and Stopping Node Manager	20-3
20.1.5.1	Starting Node Manager	20-3
20.1.5.2	Stopping Node Manager	20-4
20.1.5.3	Starting Node Manager for an Administration Server	20-4
20.1.6	Starting, Stopping, and Restarting WebLogic Administration Server	20-4
20.1.6.1	Starting WebLogic Administration Server	20-4
20.1.6.2	Stopping WebLogic Administration Server	20-4
20.1.6.3	Restarting WebLogic Administration Server	20-5
20.1.7	Starting, Stopping, and Restarting Oracle Identity Manager	20-5
20.1.7.1	Starting Oracle Identity Manager	20-5
20.1.7.2	Stopping Oracle Identity Manager	20-5
20.1.7.3	Restarting Oracle Identity Manager	20-5
20.1.8	Starting, Stopping, and Restarting Oracle Access Manager Managed Servers	20-6
20.1.8.1	Starting Oracle Access Manager Managed Servers	20-6
20.1.8.2	Stopping Oracle Access Manager Managed Servers	20-6
20.1.8.3	Restarting Oracle Access Manager Managed Servers	20-6
20.1.9	Starting and Stopping Oracle Identity Federation Managed Servers	20-6
20.1.9.1	Starting Oracle Identity Federation	20-6
20.1.9.2	Stopping Oracle Identity Federation	20-7
20.1.9.3	Restarting Oracle Identity Federation	20-7
20.1.9.4	Starting the EMAgent	20-7
20.1.9.5	Stopping the Oracle Identity Federation Instances and EMAgent	20-7
20.2	About Identity Management Console URLs	20-7
20.3	Monitoring Enterprise Deployments	20-8
20.3.1	Monitoring Oracle Internet Directory	20-8
20.3.1.1	Oracle Internet Directory Component Names Assigned by Oracle Identity Manager Installer	20-8
20.3.2	Monitoring Oracle Virtual Directory	20-9
20.3.3	Monitoring WebLogic Managed Servers	20-9
20.4	Scaling Enterprise Deployments	20-10
20.4.1	Scaling Up the Topology	20-10
20.4.1.1	Scaling Up the Directory Tier	20-10
20.4.1.1.1	Scaling Up Oracle Internet Directory	20-10
20.4.1.1.2	Scaling Up Oracle Virtual Directory	20-11
20.4.1.2	Scaling Up the Application Tier	20-11
20.4.1.2.1	Scaling Up ODSM	20-12
20.4.1.2.2	Scaling Up Oracle Access Manager 11g	20-12
20.4.1.2.3	Scaling Up Oracle Identity Manager (Adding Managed Servers to Existing Nodes)	20-15
20.4.1.2.4	Scaling Up Oracle Identity Federation	20-19
20.4.1.3	Scaling Up the Web Tier	20-20
20.4.2	Scaling Out the Topology	20-20
20.4.2.1	Scaling Out the Directory Tier	20-20
20.4.2.1.1	Scaling Out Oracle Internet Directory	20-21

20.4.2.1.2	Scaling Out Oracle Virtual Directory	20-21
20.4.2.2	Scaling Out the Application Tier	20-21
20.4.2.2.1	Scaling Out Oracle Identity Federation	20-22
20.4.2.2.2	Scaling Out ODSM	20-22
20.4.2.2.3	Scaling Out Oracle Access Manager 11g	20-22
20.4.2.2.4	Scaling Out Oracle Identity Manager (Adding Managed Servers to New Nodes)	20-26
20.4.2.3	Scaling Out the Web Tier	20-33
20.5	Auditing Identity Management	20-33
20.6	Performing Backups and Recoveries	20-36
20.7	Patching Enterprise Deployments	20-37
20.7.1	Patching an Oracle Fusion Middleware Source File	20-37
20.7.2	Patching Identity and Access Management in a Single Domain Topology	20-37
20.7.3	Patching Identity and Access Management in a Split Domain Topology	20-38
20.7.4	Patching Identity Management Components	20-38
20.8	Preventing Timeouts for SQL	20-39
20.9	Troubleshooting	20-39
20.9.1	Troubleshooting Oracle Internet Directory	20-39
20.9.1.1	Oracle Internet Directory Server is Not Responsive.	20-40
20.9.1.2	SSO/LDAP Application Connection Times Out	20-40
20.9.1.3	LDAP Application Receives LDAP Error 53 (DSA Unwilling to Perform)	20-40
20.9.1.4	TNSNAMES.ORA, TAF Configuration, and Related Issues	20-40
20.9.2	Troubleshooting Oracle Virtual Directory	20-40
20.9.2.1	Command Not Found Error When Running SSLServerConfig.sh	20-41
20.9.2.2	Oracle Virtual Directory is Not Responsive	20-41
20.9.2.3	SSO/LDAP Application Connection Times Out	20-41
20.9.2.4	TNSNAMES.ORA, TAF Configuration, and Related Issues	20-41
20.9.2.5	SSLServerConfig.sh Fails with Error	20-42
20.9.3	Troubleshooting Oracle Directory Services Manager	20-42
20.9.3.1	ODSM Browser Window and Session Issues	20-42
20.9.3.2	ODSM Does not Open When Invoked from Fusion Middleware Control	20-43
20.9.3.3	ODSM Failover is Not Transparent	20-43
20.9.3.4	ODSM Loses Connection and Displays Message that LDAP Server is Down	20-44
20.9.3.5	ODSM Loses Connection to Instance Using ORAC Database	20-44
20.9.3.6	OHS Must Be Configured to Route ODSM Requests to Multiple Oracle WebLogic Servers	20-44
20.9.3.7	ODSM is Not Accessible	20-45
20.9.4	Troubleshooting Oracle Access Manager 11g	20-45
20.9.4.1	Fusion Applications Preverify Fails to Validate OAM Admin Users	20-46
20.9.4.2	User Reaches the Maximum Allowed Number of Sessions	20-46
20.9.4.3	Policies Do Not Get Created When Oracle Access Manager is First Installed	20-46
20.9.4.4	You Are Not Prompted for Credentials After Accessing a Protected Resource	20-47
20.9.4.5	Cannot Log In to OAM Console	20-47
20.9.4.6	Unable to Create Keystore – Unable to Load Key	20-48
20.9.4.7	Error When Starting OAM Managed Servers on Windows	20-48
20.9.5	Troubleshooting Oracle Identity Manager	20-48

20.9.5.1	java.io.FileNotFoundException When Running Oracle Identity Manager Configuration	20-49
20.9.5.2	ResourceConnectionValidationxception When Creating User in Oracle Identity Manager	20-49
20.9.6	Troubleshooting Oracle Identity Federation	20-49
20.9.6.1	Cannot Log In to the Oracle Identity Federation Server (Windows)	20-50
20.9.6.2	Extending the Domain with Oracle Identity Federation Fails	20-50
20.9.6.3	Cannot Change Oracle Identity Federation Parameters by Using Fusion Middleware Control	20-50

Index

List of Figures

2-1	Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications.	2-3
2-2	Split Domain Topology	2-4
2-3	Oracle Identity Federation 11g Topology.....	2-5
2-4	Flow Chart of the Oracle Identity Management Enterprise Deployment Process for Oracle Fusion Applications	2-13
3-1	IPs and VIPs Mapped to Administration Server and Managed Servers	3-9
3-2	IPs and VIPs Mapped to Administration Server and Managed Servers: Split Domain Topology	3-10
4-1	Directory Structure for Identity Management.....	4-7
4-2	Directory Structure for Identity Management Split Domain Topology	4-8
20-1	Audit Event Flow	20-34

List of Tables

2-1	Typical Hardware Requirements	2-10
2-2	Software Versions Used	2-11
2-3	Steps in the Oracle Identity Management Enterprise Deployment Process	2-14
3-1	Load Balancer Configuration	3-6
3-2	Virtual Hosts.....	3-10
3-3	Ports Used in the Oracle Identity Management Enterprise Deployment topologies ...	3-11
4-1	Local Storage Directories	4-4
4-2	Volumes on Shared Storage, Single Domain Topology	4-4
4-3	Volumes on Shared Storage, Split Domain Topology	4-5
4-4	Directory Structure Elements.....	4-8
5-1	Mapping between Topologies, Databases and Schemas.....	5-2
5-2	Required Patches for Oracle Database 11g (11.1.0.7)	5-3
5-3	Required Patches for Oracle Database 11g (11.2.0.2.0)	5-4
5-4	Minimum Initialization Parameters for Oracle RAC Databases.....	5-4
5-5	Minimum Initialization Parameters for Oracle RAC Oracle Internet Directory Databases ...	5-5
5-6	Component Schemas	5-9
6-1	Software to be Installed for Different Topologies	6-2
6-2	Summary of Homes.....	6-6
8-1	Steps for Creating a WebLogic Domain	8-2
8-2	URLs Available Prior to Web Tier Integration	8-2
8-3	URLs Available After Web Tier Integration	8-3
8-4	Virtual Hosts for Single or Split Domain.....	8-3
8-5	Domains to be Created.....	8-4
8-6	Clusters.....	8-10
8-7	Servers to Assign to Clusters.....	8-10
13-1	OAM URLs Before Web Tier Configuration.....	13-2
13-2	OAM URLs After Web Tier Configuration.....	13-2
13-3	Host Name and Port Values.....	13-10
14-1	OIM URLs	14-2
16-1	Hosts in Each Topology	16-1
17-1	Files Required for the PATH Environment Variable.....	17-5
17-2	WLS_OIM1, WLS_OIM2, WLS_SOA1, WLS_SOA2 Server Migration.....	17-7
20-1	Console URLs	20-7
20-2	Static Artifacts to Back Up in the Identity Management Enterprise Deployment	20-36
20-3	Run-Time Artifacts to Back Up in the Identity Management Enterprise Deployments	20-37

Preface

This preface describes the audience, contents and conventions used in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Fusion Applications Edition)*.

Audience

This guide is intended for system administrators who are responsible for installing and configuring Oracle Identity Management enterprise deployments for Oracle Fusion Applications.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Related Documents

The following manuals in the Oracle Fusion Middleware documentation library provide additional information on the process of installing and configuring the Enterprise Deployment architecture:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*
- *Oracle Fusion Middleware Administrator's Guide*
- *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite*
- *Oracle Fusion Middleware Application Security Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Directory Integration Platform*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*
- *Oracle Fusion Middleware Integration Guide for Oracle Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Federation*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Linux*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Solaris Operating System*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for HP-UX*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for hp Tru64 UNIX*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for AIX Based Systems*
- *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide for Microsoft Windows*
- *Oracle Database Backup and Recovery User's Guide*
- *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite*

For additional information about Oracle Fusion Applications, consult the following documents in the Oracle Fusion Applications 11.1.4 library:

- *Oracle Fusion Applications Administrator and Implementor Roadmap*
- *Oracle Fusion Applications Administrator's Guide*
- *Oracle Fusion Applications Customer Relationship Management Enterprise Deployment Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide

The following topics introduce the new and changed features of Oracle Identity and Access management and other significant changes that are described in this guide, and provides pointers to additional information.

New and Changed Features for 11g Release 5 (11.1.5)

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition) 11g Release 5 (11.1.5) includes the following chapter, which was not included in the previous release:

- Extending the Domain to Include Oracle Identity Federation. See [Chapter 15](#).

Other chapters have also been updated to include information about Oracle Identity Federation.

Enterprise Deployment Overview

This chapter provides an overview of the enterprise topology for Oracle Identity Management.

This chapter contains the following sections:

- [Section 1.1, "About the Enterprise Deployment Guide"](#)
- [Section 1.2, "Enterprise Deployment Terminology"](#)
- [Section 1.3, "Benefits of Oracle Recommendations"](#)

Oracle Identity Management presents a comprehensive suite of products for all aspects of identity management. This guide describes reference enterprise topologies for the Oracle Identity Management Infrastructure components of Oracle Fusion Middleware. It also provides detailed instructions and recommendations to create the topologies by following the enterprise deployment guidelines.

Deploying Oracle Identity Management as described in this guide is a prerequisite for deploying Oracle Fusion Applications as described in *Oracle Fusion Applications Customer Relationship Management Enterprise Deployment Guide*.

1.1 About the Enterprise Deployment Guide

An enterprise deployment is an Oracle best practices blueprint based on proven Oracle high-availability technologies and recommendations for Oracle Fusion Middleware. The high-availability best practices described in this book make up one of several components of high-availability best practices for all Oracle products across the entire technology stack—Oracle Database, Oracle Fusion Middleware, Oracle Applications, Oracle Collaboration Suite, and Oracle Grid Control.

An Oracle Fusion Middleware enterprise deployment:

- Considers various business service level agreements (SLA) to make high-availability best practices as widely applicable as possible
- Leverages database grid servers and storage grid with low-cost storage to provide highly resilient, lower cost infrastructure
- Uses results from extensive performance impact studies for different configurations to ensure that the high-availability architecture is optimally configured to perform and scale to business needs
- Enables control over the length of time to recover from an outage and the amount of acceptable data loss from a natural disaster
- Evolves with each Oracle version and is completely independent of hardware and operating system

For more information on high availability practices, see the Oracle Database High Availability page on Oracle Technology Network at:

<http://www.oracle.com/technetwork/database/features/availability/index-087701.html>

Note: The Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition) focuses on enterprise deployments in Linux environments. However, you can also implement enterprise deployments using UNIX and Windows environments.

1.2 Enterprise Deployment Terminology

This section identifies enterprise deployment terminology used in the guide.

- **Oracle home:** An Oracle home contains installed files necessary to host a specific product. For example, the SOA Oracle home contains a directory that contains binary and library files for Oracle SOA Suite. An Oracle home resides within the directory structure of the Middleware home. Each Oracle home can be associated with multiple Oracle instances or Oracle WebLogic Server domains.
- **Oracle Common home:** This environment variable and related directory path refers to the Oracle home that contains the binary and library files required for the Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).
- **WebLogic Server home:** A WebLogic Server home contains installed files necessary to host a WebLogic Server. The WebLogic Server home directory is a peer of Oracle home directories and resides within the directory structure of the Middleware home.
- **Middleware home:** A Middleware home consists of the Oracle WebLogic Server home, and, optionally, one or more Oracle homes. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through NFS.
- **Oracle instance:** An Oracle instance contains one or more active middleware system components, for example Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. You determine which components are part of an instance, either at install time or by creating and configuring an instance at a later time. An Oracle instance contains files that can be updated, such as configuration files, log files, temporary files.
- **failover:** When a member of a high availability system fails unexpectedly (unplanned downtime), in order to continue offering services to its consumers, the system undergoes a failover operation. If the system is an active-passive system, the passive member is activated during the failover operation and consumers are directed to it instead of the failed member. The failover process can be performed manually, or it can be automated by setting up hardware cluster services to detect failures and move cluster resources from the failed node to the standby node. If the system is an active-active system, the failover is performed by the load balancer entity serving requests to the active members. If an active member fails, the load balancer detects the failure and automatically redirects requests for the failed member to the surviving active members. See *Oracle Fusion Middleware High Availability Guide* for information on active-active and active-passive systems.
- **failback:** After a system undergoes a successful failover operation, the original failed member can be repaired over time and be re-introduced into the system as a

standby member. If desired, a failback process can be initiated to activate this member and deactivate the other. This process reverts the system back to its pre-failure configuration.

- **hardware cluster:** A hardware cluster is a collection of computers that provides a single view of network services (for example: an IP address) or application services (for example: databases, Web servers) to clients of these services. Each node in a hardware cluster is a standalone server that runs its own processes. These processes can communicate with one another to form what looks like a single system that cooperatively provides applications, system resources, and data to users.

A hardware cluster achieves high availability and scalability through the use of specialized hardware (cluster interconnect, shared storage) and software (health monitors, resource monitors). (The cluster interconnect is a private link used by the hardware cluster for heartbeat information to detect node death.) Due to the need for specialized hardware and software, hardware clusters are commonly provided by hardware vendors such as Sun, HP, IBM, and Dell. While the number of nodes that can be configured in a hardware cluster is vendor dependent, for the purpose of Oracle Fusion Middleware high availability, only two nodes are required. Hence, this document assumes a two-node hardware cluster for high availability solutions employing a hardware cluster.

- **cluster agent:** The software that runs on a node member of a hardware cluster that coordinates availability and performance operations with other nodes. Clusterware provides resource grouping, monitoring, and the ability to move services. A cluster agent can automate the service failover.
- **clusterware:** A software that manages the operations of the members of a cluster as a system. It allows one to define a set of resources and services to monitor via a heartbeat mechanism between cluster members and to move these resources and services to a different member in the cluster as efficiently and transparently as possible.
- **shared storage:** Shared storage is the storage subsystem that is accessible by all the machines in the enterprise deployment domain. Among other things, the following are located on the shared disk:
 - Middleware Home software
 - AdminServer Domain Home
 - JMS
 - Tlogs (where applicable)

Managed Server homes can also be optionally located in the shared disk. The shared storage can be a Network Attached Storage (NAS), a Storage Area Network (SAN) or any other storage system that multiple nodes can access simultaneously and can read-write.

- **primary node:** The node that is actively running an Oracle Fusion Middleware instance at any given time and has been configured to have a backup/secondary node. If the primary node fails, Oracle Fusion Middleware instance is failed over to the secondary node. This failover can be manual or automated using the Clusterware for Administration Server. For a server migration based scenario, WebLogic Whole Server Migration is used for automated failover.
- **secondary node:** The node that is the backup node for an Oracle Fusion Middleware instance. This is where the active instance fails over when the

primary node is no longer available. See the definition for primary node in this section.

- **network host name:** Network host name is a name assigned to an IP address either through the `/etc/hosts` file or through DNS resolution. This name is visible in the network that the machine to which it refers to is connected. Often, the network host name and physical host name are identical. However, each machine has only one physical host name but may have multiple network host names. Thus, a machine's network host name may not always be its physical host name.
- **physical host name:** This guide differentiates between the terms physical host name and network host name. This guide uses physical host name to refer to the "internal name" of the current machine. On Linux, this is the name returned by the `hostname` command.

Physical host name is used by Oracle Fusion Middleware to reference the local host. During installation, the installer automatically retrieves the physical host name from the current machine and stores it in the Oracle Fusion Middleware configuration metadata on disk.

- **physical IP:** Physical IP refers to the IP of a machine on the network. In almost all cases, it is normally associated with the physical host name of the machine (see the definition of the physical host name). In contrast to a virtual IP, it is always associated with the same machine when on a network.
- **switchover:** During normal operation, active members of a system may require maintenance or upgrading. A switchover process can be initiated to allow a substitute member to take over the workload performed by the member that requires maintenance or upgrading, which undergoes planned downtime. The switchover operation ensures continued service to consumers of the system.
- **switchback:** When a switchover operation is performed, a member of the system is deactivated for maintenance or upgrading. When the maintenance or upgrading is completed, the system can undergo a switchback operation to activate the upgraded member and bring the system back to the pre-switchover configuration.
- **virtual host name:** Virtual host name is a network addressable host name that maps to one or more physical machines via a load balancer or a hardware cluster. For load balancers, the name "virtual server name" is used interchangeably with virtual host name in this book. A load balancer can hold a virtual host name on behalf of a set of servers, and clients communicate indirectly with the machines using the virtual host name. A virtual host name in a hardware cluster is a network host name assigned to a cluster virtual IP. Because the cluster virtual IP is not permanently attached to any particular node of a cluster, the virtual host name is not permanently attached to any particular node either.

Note: Whenever the term "virtual host name" is used in this document, it is assumed to be associated with a virtual IP address. In cases where just the IP address is needed or used, it will be explicitly stated.

- **virtual IP:** Also, cluster virtual IP and load balancer virtual IP. Generally, a virtual IP can be assigned to a hardware cluster or load balancer. To present a single system view of a cluster to network clients, a virtual IP serves as an entry point IP address to the group of servers which are members of the cluster. A virtual IP can be assigned to a server load balancer or a hardware cluster.

A hardware cluster uses a cluster virtual IP to present to the outside world the entry point into the cluster (it can also be set up on a standalone machine). The hardware cluster's software manages the movement of this IP address between the two physical nodes of the cluster while clients connect to this IP address without the need to know which physical node this IP address is currently active on. In a typical two-node hardware cluster configuration, each machine has its own physical IP address and physical host name, while there could be several cluster IP addresses. These cluster IP addresses float or migrate between the two nodes. The node with current ownership of a cluster IP address is active for that address.

A load balancer also uses a virtual IP as the entry point to a set of servers. These servers tend to be active at the same time. This virtual IP address is not assigned to any individual server but to the load balancer which acts as a proxy between servers and their clients.

These will be described in more detail in the following chapters.

1.3 Benefits of Oracle Recommendations

The Oracle Fusion Middleware configurations discussed in this guide are designed to ensure security of all transactions, maximize hardware resources, and provide a reliable, standards-compliant system for enterprise computing with a variety of applications. The security and high availability benefits of the Oracle Fusion Middleware configurations are realized through isolation in firewall zones and replication of software components.

This section contains the following topics:

- [Section 1.3.1, "Built-in Security"](#)
- [Section 1.3.2, "High Availability"](#)

1.3.1 Built-in Security

The Enterprise Deployment architectures are secure because every functional group of software components is isolated in its own DMZ, and all traffic is restricted by protocol and port. The following characteristics ensure security at all needed levels, as well as a high level of standards compliance:

- All external communication received on port 80 is redirected to port 443.
- External communication uses the Secure Socket Layer (SSL) secure Web Protocol. This is terminated at the site's load balancer.
- Communication from external clients does not go beyond the Load Balancing Router level.
- No direct communication from the Load Balancing Router to the data tier DMZ is allowed.
- Components are separated between DMZs on the web tier, application tier, and the directory tier.
- Direct communication across two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- Oracle Internet Directory is isolated in the directory tier DMZ.
- Identity Management components are in the application tier DMZ.

- All communication between components across DMZs is restricted by port and protocol, according to firewall rules.

1.3.2 High Availability

The Enterprise Deployment architectures are highly available, because each component or functional group of software components is replicated on a different computer, and configured for component-level high availability.

Introduction to the Enterprise Deployment Reference Topologies

This chapter describes and illustrates the enterprise deployment reference topologies described in this guide. The road map for installation and configuration directs you to the appropriate chapters for the tasks you need to perform. Use this chapter to help you plan your Oracle Identity Management enterprise deployment.

This chapter contains the following topics:

- [Section 2.1, "Overview of Enterprise Deployment Reference Topologies"](#)
- [Section 2.2, "Hardware Requirements for an Enterprise Deployment"](#)
- [Section 2.3, "Identifying the Software Components to Install"](#)
- [Section 2.4, "Road Map for the Reference Topology Installation and Configuration"](#)

2.1 Overview of Enterprise Deployment Reference Topologies

This section describes diagrams used to illustrate the enterprise deployment possibilities described in this guide. Use this section to plan your enterprise deployment topology.

This section covers these topics:

- [Section 2.1.1, "Reference Topologies Documented in the Guide"](#)
- [Section 2.1.2, "About the Directory Tier"](#)
- [Section 2.1.3, "About the Application Tier"](#)
- [Section 2.1.4, "About the Web Tier"](#)

2.1.1 Reference Topologies Documented in the Guide

Oracle Identity Management consists of a number of products, which can be used either individually or collectively. The Enterprise Deployment Guide for Identity Management (Fusion Applications Edition) enables you to build two different enterprise topologies for Fusion Applications.

One of the topologies shown is the split domain topology. A split domain topology is useful if you need either of the following features:

- The ability to keep operational functionality (OAM) separate from administrative (OIM) functions
- The ability to patch OIM independently

This section provides diagrams of the topologies.

In the diagrams, active nodes are shown in color, and passive nodes are shown in white.

See Also: supported platforms documentation for Oracle Fusion Applications.

This section contains the following topics:

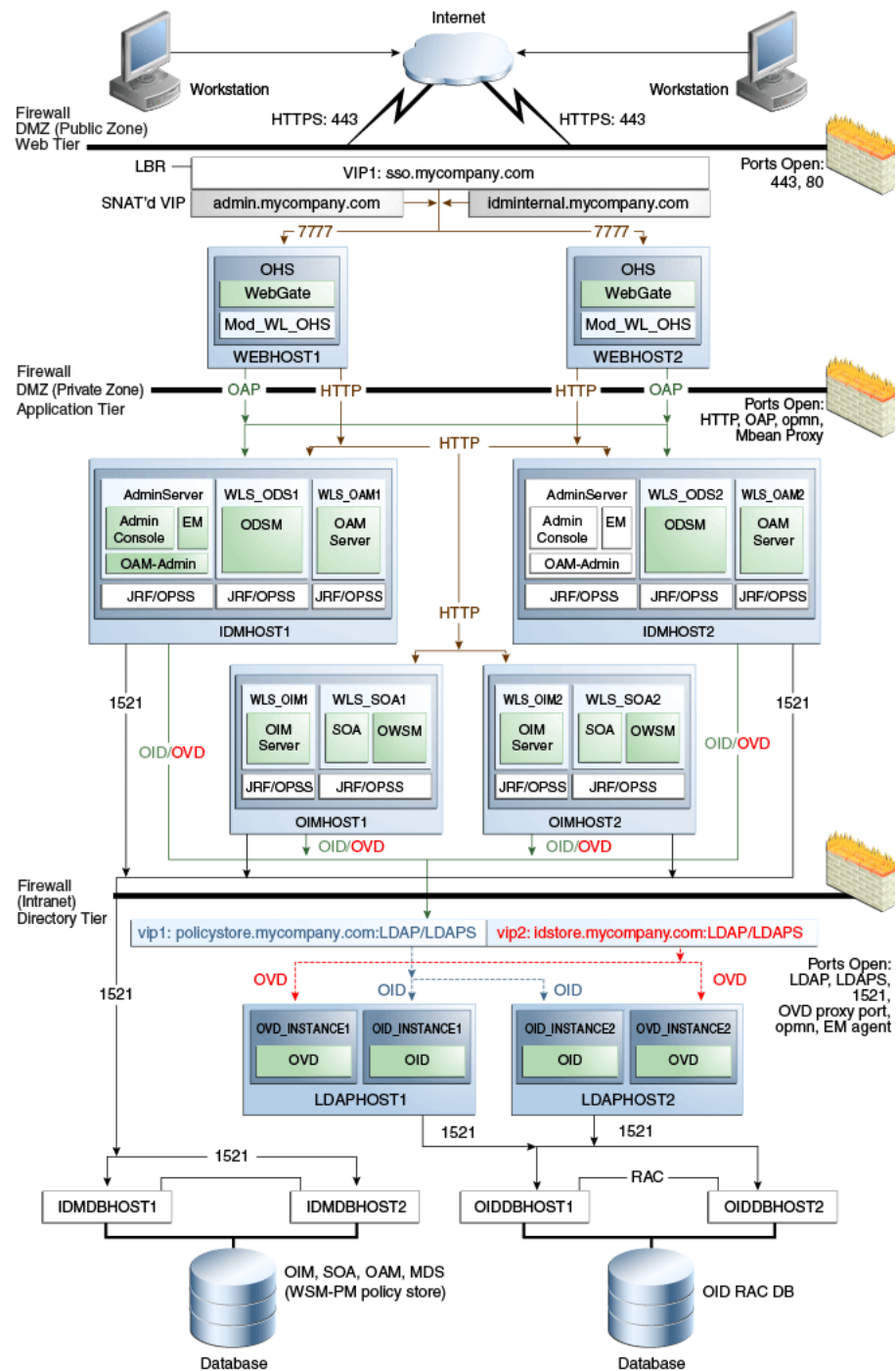
- [Section 2.1.1.1, "Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications"](#)
- [Section 2.1.1.2, "Split Domain Topology for Oracle Fusion Applications"](#)
- [Section 2.1.1.3, "Oracle Identity Federation 11g for Fusion Applications"](#)

Note: Customers who use machines with large memory and CPU foot prints can collapse multiple machines in the topology into single machines within the same tier. For example, IDMHOST and OIMHOST can be collapsed into single host

2.1.1.1 Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications

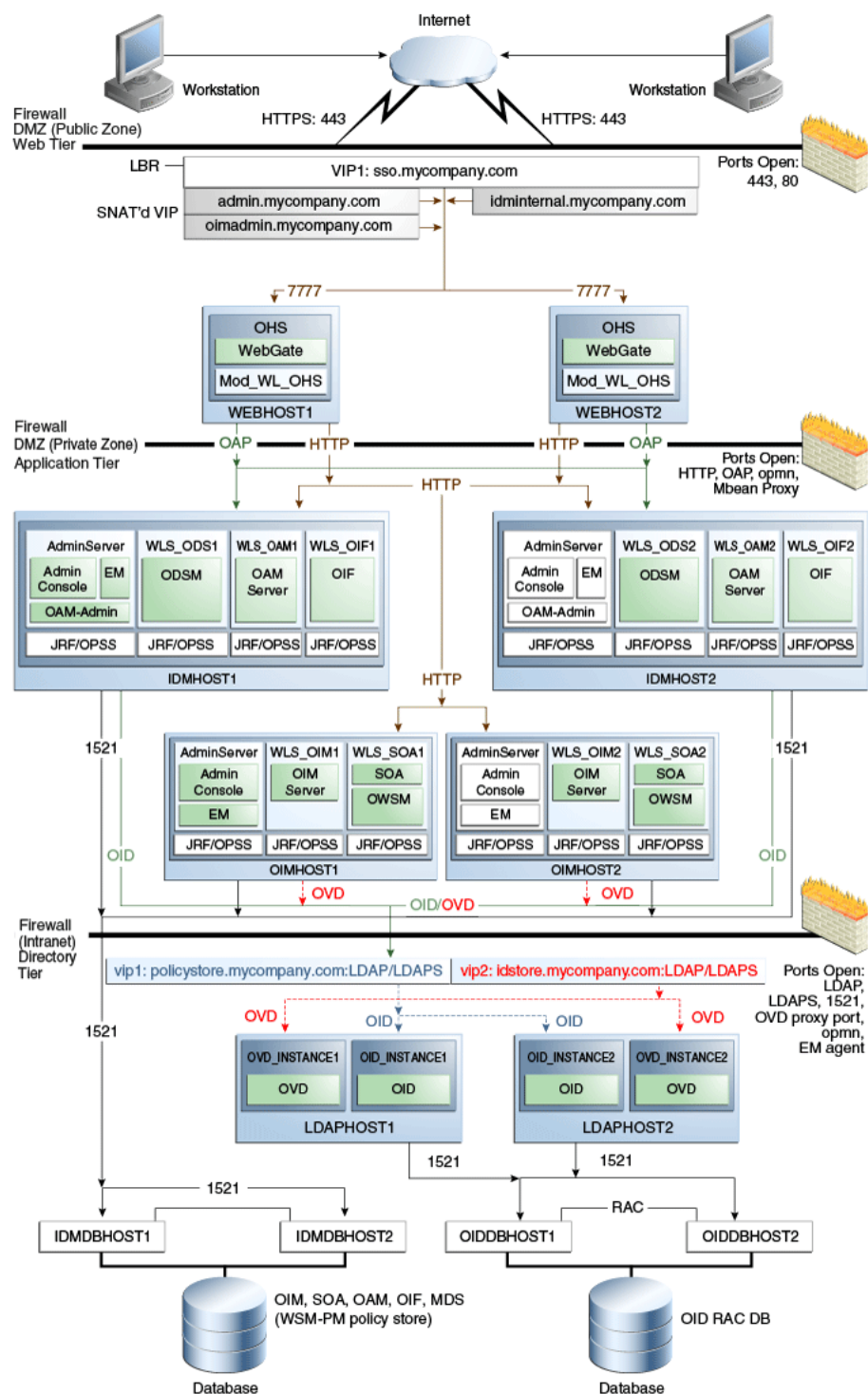
[Figure 2–1](#) is a diagram of the Oracle Access Manager 11g and Oracle Identity Manager 11g topology.

Figure 2–1 Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications



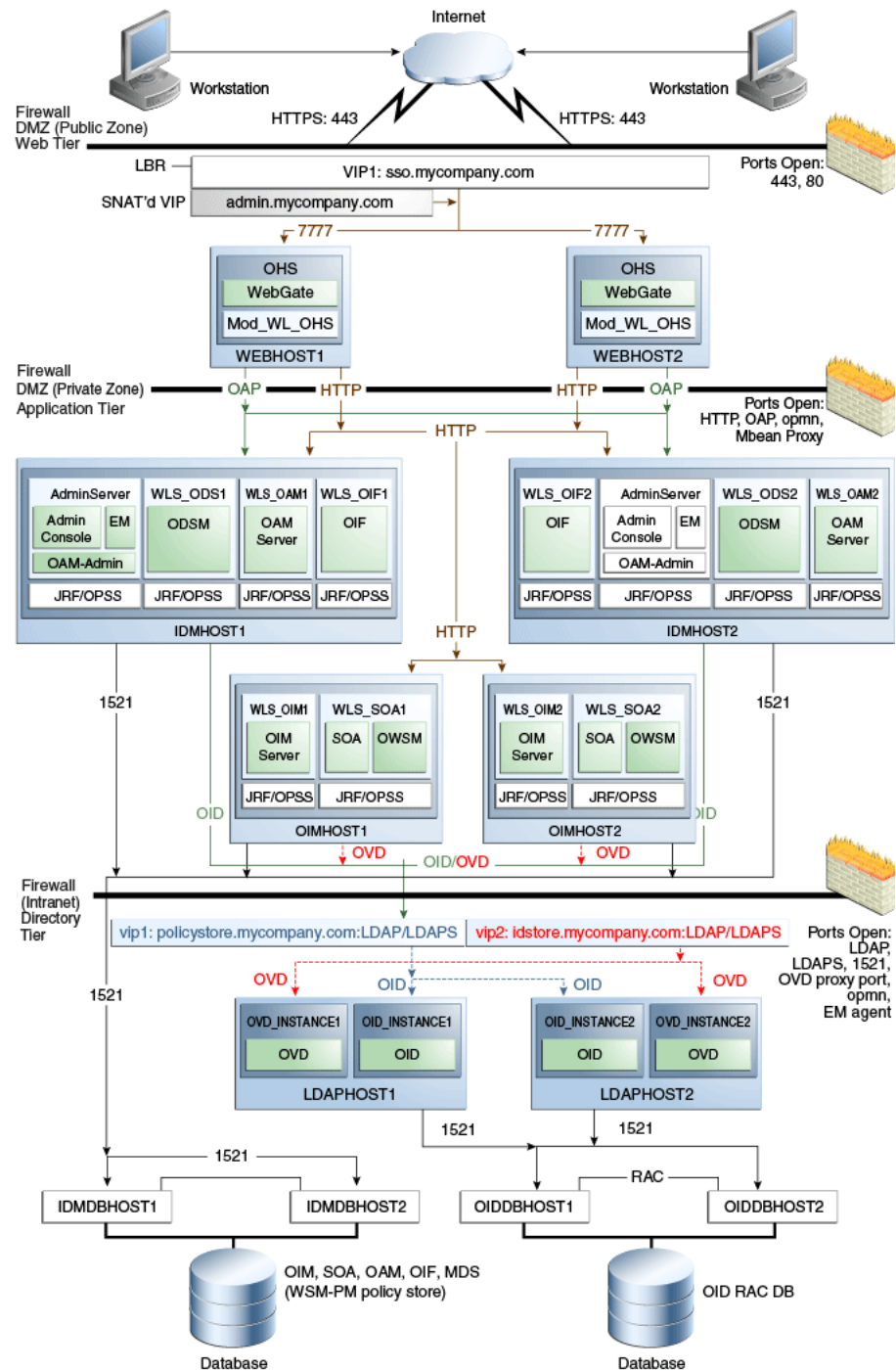
2.1.1.2 Split Domain Topology for Oracle Fusion Applications

Figure 2–2 is a diagram of the split domain topology for Oracle Fusion Applications, where Oracle Identity Management is placed in a separate domain.

Figure 2–2 Split Domain Topology

2.1.1.3 Oracle Identity Federation 11g for Fusion Applications

Figure 2–3 is a diagram of the Oracle Identity Federation 11 g topology for Fusion Applications.

Figure 2–3 Oracle Identity Federation 11g Topology

2.1.2 About the Directory Tier

The directory tier is in the Intranet Zone. The directory tier is the deployment tier where all the LDAP services reside. This tier includes products such as Oracle Internet Directory and Oracle Virtual Directory. The directory tier is managed by directory administrators providing enterprise LDAP service support.

The directory tier is closely tied with the data tier. Access to the data tier is important for the following reasons:

- Oracle Internet Directory relies on Oracle Database as its back end.
- Oracle Virtual Directory provides virtualization support for other LDAP services or databases or both.

In some cases, the directory tier and data tier might be managed by the same group of administrators. In many enterprises, however, database administrators own the data tier while directory administrators own the directory tier.

Typically protected by firewalls, applications above the directory tier access LDAP services through a designated LDAP host port. The standard LDAP port is 389 for the non-SSL port and 636 for the SSL port. LDAP services are often used for white pages lookup by clients such as email clients in the intranet. The ports 389 and 636 on the load balancer are typically redirected to the non-privileged ports used by the individual directory instances.

The directory tier stores two types of information:

- Identity Information: Information about users and groups
- Oracle Platform Security Services (OPSS): Information about security policies and about configuration.

Although the topology diagrams do not show LDAP directories other than Oracle Internet Directory, you can use Microsoft Active Directory to store identity information. You must always store policy information in Oracle Internet Directory. You may store identity information in Oracle Internet Directory or in another directory.

If you store the Identity details in a directory other than Oracle Internet Directory, you can use Oracle Virtual Directory to present that information

Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite describes how to configure Oracle Virtual Directory for two multidirectory scenarios.

- A split profile, or split directory configuration, is one where identity data is stored in multiple directories, possibly in different locations. A split profile is used to store custom attributes required for Fusion Application Deployment. Use this kind of deployment when you do not want to modify the existing Identity Store by extending the schema. In that case, deploy a new Oracle Internet Directory instance to store the extended attributes. Alternatively, you can use the Oracle Internet Directory instance deployed for Policy Store for this purpose.
- Another multidirectory scenario is one where you have distinct user and group populations. In this configuration, Oracle-specific entries and attributes are stored in Oracle Internet Directory. Enterprise-specific entries that might have Fusion Applications-specific attributes are stored in Active Directory.

In both multidirectory scenarios, you use Oracle Virtual Directory to present all the identity data in a single consolidated view that Oracle Identity Management components can interpret.

Although you can use a single Oracle Internet Directory instance for storing both the identity and policy information, in some cases you might need to use two separate Oracle Internet Directory installations, one for the Policy Store and another for Identity Store. For example, this might be necessary due to throughput or enterprise directory requirements. You might also need to use separate Oracle Internet Directory installations if you have a shared Identity Management deployment with multiple Oracle Fusion Applications pods pointing to it.

If you intend to separate your identity and policy information, you must create two separate clusters of highly available Oracle Internet Directory. These Oracle Internet

Directory clusters can share the same machines but they should use separate Real Application Clusters databases as their data store.

If you are using Oracle Internet Directory exclusively, you do not need to use Oracle Virtual Directory.

This guide assumes that you are creating two virtual names: one for your Policy Store (`polycystore.mycompany.com`) and one for your Identity Store (`idstore.mycompany.com`). When using a single Oracle Internet Directory for both your identity and policy information, you can either create two virtual host names, both pointing to the same directory, or combine them into a single suitable virtual host name in the load balancer.

If you are using Oracle Internet Directory as your Identity Store, you can configure it to use multimaster replication as described in the *Oracle Fusion Middleware High Availability Guide* chapter Configuring Identity Management for Maximum High Availability. This enables you to maintain the same naming contexts on multiple directory servers. It can improve performance by providing more servers to handle queries and by bringing the data closer to the client. It improves reliability by eliminating risks associated with a single point of failure.

2.1.2.1 High Availability Provisions

- Oracle Internet Directory Instances are active/active deployments.
- Oracle Virtual Directory Instances are active/active deployments.
- If the Oracle Internet Directory fails on the LDAPHOST, Oracle Process Management and Notification (OPMN) server attempts to restart it.
- If the Oracle Virtual Directory fails on the LDAPHOST, Oracle Process Management and Notification (OPMN) server attempts to restart it.

2.1.3 About the Application Tier

The application tier is the tier where Java EE applications are deployed. Products such as Oracle Identity Manager, Oracle Identity Federation, Oracle Directory Services Manager and Oracle Enterprise Manager Fusion Middleware Control are the key Java EE components that can be deployed in this tier. Applications in this tier benefit from the High Availability support of Oracle WebLogic Server.

The Identity Management applications in the application tier interact with the directory tier as follows:

- They leverage the directory tier for enterprise identity information.
- In some cases, they leverage the directory tier (and sometimes the database in the data tier) for application metadata.
- Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager are administration tools that provide administrative functionalities to the components in the application tier as well as the directory tier.
- WebLogic Server has built-in web server support. If enabled, the HTTP listener exists in the application tier as well. However, for the enterprise deployment shown in Figure 1-1, customers have a separate web tier relying on web servers such as Apache or Oracle HTTP Server.

In the application tier:

- IDMHOST1 and IDMHOST2 have the WebLogic Server with the Administration Console, Oracle Enterprise Manager Fusion Middleware Control, Oracle Directory Services Manager, Oracle Identity Federation, and Oracle Access Management Server configured. IDMHOST1 and IDMHOST2 run both the WebLogic Server Administration Servers and Managed Servers. Note that the Administration Server is configured to be active-passive, that is, although it is installed on both nodes, only one instance is active at any time. If the active instance goes down, then the passive instance starts up and becomes the active instance.

The Oracle Access Management Server communicates with the directory tier to verify user information.

- On the firewall protecting the application tier, the HTTP ports, and OAP port are open. The OAP (Oracle Access Protocol) port is for the WebGate module running in Oracle HTTP Server in the web tier to communicate with Oracle Access Manager to perform operations such as user authentication.
- In the OAM and OIM topology, OIMHOST1 and OIMHOST2 have Oracle Identity Manager and Oracle SOA installed. Oracle Identity Manager is user provisioning application. Oracle SOA deployed in this topology is exclusively used for providing workflow functionality for Oracle Identity Manager.

2.1.3.1 Architecture Notes

- Oracle Enterprise Manager Fusion Middleware Control is integrated with Oracle Access Manager using the Oracle Platform Security Services (OPSS) agent.
- The Oracle WebLogic Server console, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Access Management console are always bound to the listen address of the Administration Server.
- The WebLogic administration server is a singleton service. It runs on only one node at a time. In the event of failure, it is restarted on a surviving node.
- The WLS_ODS1 Managed Server on IDMHOST1 and WLS_ODS2 Managed Server on IDMHOST2 are in a cluster and the Oracle Directory Services Manager applications are targeted to the cluster.
- The WLS_OAM1 Managed Server on IDMHOST1 and WLS_OAM2 Managed Server on IDMHOST2 are in a cluster and the Oracle Access Manager applications are targeted to the cluster.
- Oracle Directory Services Manager are bound to the listen addresses of the WLS_ODS1 and WLS_ODS2 Managed Servers. By default, the listen address for these Managed Servers is set to IDMHOST1 and IDMHOST2 respectively.
- The WLS_OIM1 Managed Server on OIMHOST1 and WLS_OIM2 Managed Server on OIMHOST2 are in a cluster and the Oracle Identity Manager applications are targeted to the cluster.
- The WLS_SOA1 Managed Server on OIMHOST1 and WLS_SOA2 Managed Server on OIMHOST2 are in a cluster and the Oracle SOA applications are targeted to the cluster.
- The WLS_OIF1 Managed Server on IDMHOST1 and WLS_OIF2 Managed Server on IDMHOST2 are in a cluster and the Oracle Identity Federation applications are targeted to the cluster.
- In the OIM split domain topology, Oracle Identity Manager components are installed into a separate domain.

2.1.3.2 High Availability Provisions

- The OAM Servers are active-active deployments.
- Oracle Access Manager, Oracle Identity Manager, and SOA are active-active deployments; these servers communicate with the data tier at run time.
- The WebLogic Administration Server and Oracle Enterprise Manager deployment is active-passive (where other components are active-active). There is one Administration Server per domain.
- The Identity Federation Servers are active-active deployments; the Oracle Identity Federation Server may communicate with the data tier at run time.
- The WebLogic Administration Server is a singleton component deployed in an active-passive configuration. If the primary fails or the Administration Server on IDMHOST1 does not start, the Administration Server on the secondary host can be started. If a WebLogic managed server fails, the node manager running on that host attempts to restart it.

2.1.3.3 Security Provisions

Oracle WebLogic Server Console, Oracle Enterprise Manager Fusion Middleware Control console, and Oracle Access Manager Console are only accessible through a virtual host configured on the load balancer, which is only available inside the firewall.

2.1.4 About the Web Tier

The web tier is in the DMZ Public Zone. The HTTP Servers are deployed in the web tier.

Most of the Identity Management components can function without the web tier, but for most enterprise deployments, the web tier is desirable. To support enterprise level single sign-on using products such as Oracle Single Sign-On and Oracle Access Manager, the web tier is required.

While components such as Oracle Enterprise Manager Fusion Middleware Control and Oracle Directory Services Manager can function without a web tier, they can be configured to use a web tier, if desired.

In the web tier:

- WEBHOST1 and WEBHOST2 have Oracle HTTP Server, WebGate (an Access Manager component), and the `mod_wl_ohs` plug-in module installed. The `mod_wl_ohs` plug-in module enables requests to be proxied from Oracle HTTP Server to a WebLogic Server running in the application tier.
- WebGate (an Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running on IDMHOST1 and IDMHOST2, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

On the firewall protecting the web tier, the HTTP ports are 443 for HTTPS and 80 for HTTP. Port 443 is open.

2.1.4.1 Architecture Notes

Oracle HTTP Servers on WEBHOST1 and WEBHOST2 are configured with `mod_wl_ohs`, and proxy requests for the Oracle Enterprise Manager, and Oracle Directory Services Manager Java EE applications deployed in WebLogic Server on IDMHOST1 and IDMHOST2.

2.1.4.2 High Availability Provisions

If the Oracle HTTP server fails on the WEBHOST, Oracle Process Management and Notification (OPMN) server attempts to restart it.

2.1.4.3 Security Provisions

The Oracle HTTP Servers process requests received using the URLs `sso.mycompany.com` and `admin.mycompany.com`. The name `admin.mycompany.com` is only resolvable inside the firewall. This prevents access to sensitive resources such as the Oracle WebLogic Server console and Oracle Enterprise Manager Fusion Middleware Control console from the public domain.

2.2 Hardware Requirements for an Enterprise Deployment

The minimum hardware requirements for the Enterprise Deployment on Linux operating systems are listed in [Table 2–1](#). The memory figures represent the memory required to install and run an Oracle Fusion Middleware server; however, for most production sites, you should configure at least 4 GB of physical memory.

For detailed requirements, or for requirements for other platforms, see the *Oracle Fusion Middleware Installation Guide* for that platform.

Table 2–1 Typical Hardware Requirements

Server	Processor	Disk	Memory	TMP Directory	Swap
Database Hosts OIDDBHOST _n , IDMDBHOST _n	4 or more X Pentium 1.5 GHz or greater	nXm n=Number of disks, at least 4 (striped as one disk). m=Size of the disk (minimum of 30 GB)	6-16 GB	Default	Default
WEBHOST _n	2 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default
IDMHOST _n , OIMHOST _n	2 or more X Pentium 1.5 GHz or greater	10 GB	6 GB	Default	Default
Consolidated IDMHOST	4 or more X Pentium 1.5 GHz or greater	20 GB	12 GB	Default	Default
LDAPHOST _n	2 or more X Pentium 1.5 GHz or greater	10 GB	4 GB	Default	Default

These are the typical hardware requirements. For each tier, carefully consider the load, throughput, response time and other requirements to plan the actual capacity required. The number of nodes, CPUs, and memory required can vary for each tier based on the deployment profile. Production requirements may vary depending on applications and the number of users.

The Enterprise Deployment configurations described in this guide use two servers for each tier to provide failover capability; however, this does not presume adequate computing resources for any application or user population. If the system workload increases such that performance is degraded, you can add servers to the configuration by repeating the instructions for the second server (that is, WEBHOST2, IDMHOST2, LDAPHOST2, OIDDBHOST2) to install and configure additional servers where needed.

If you have powerful enough servers, you can merge IDMHOST1 and OIMHOST1 onto a single consolidated server, as shown in [Table 2–1](#). Similarly, you can merge IDMHOST2 and OIMHOST2.

Note: Oracle recommends configuring all nodes in the topology identically with respect to operating system levels, patch levels, user accounts, and user groups.

2.3 Identifying the Software Components to Install

[Table 2–2, "Software Versions Used"](#) lists the Oracle software you need to obtain before starting the procedures in this guide.

For complete information about downloading Oracle Fusion Middleware software, see [Section 6.1.2, "Software to Install"](#) and the Preparing for an Installation chapter in *Oracle Fusion Applications Installation Guide*.

Table 2–2 Software Versions Used

Short Name	Product	Version
OHS11G	Oracle HTTP Server	11.1.1.6.0
JRockit	Oracle JRockit	jrockit-jdk1.6.0_29-R28.2.0-4.0.1 or newer
WLS	Oracle WebLogic Server	10.3.6.0
IAM	Oracle Identity and Access Management	11.1.1.5.0
SOA	Oracle SOA Suite	11.1.1.6.0
IDM	Oracle Identity Management	11.1.1.6.0
WebGate 11g		11.1.1.5.0
RCU	Repository Creation Assistant	11.1.1.6.0

2.4 Road Map for the Reference Topology Installation and Configuration

Before beginning your Oracle Identity Management enterprise deployment, review the flow chart in [Figure 2–4, "Flow Chart of the Oracle Identity Management Enterprise Deployment Process for Oracle Fusion Applications"](#). This flow chart illustrates the high-level process for completing the enterprise deployment documented in this guide. [Table 2–3](#) describes the steps in the flow chart and directs you to the appropriate section or chapter for each step.

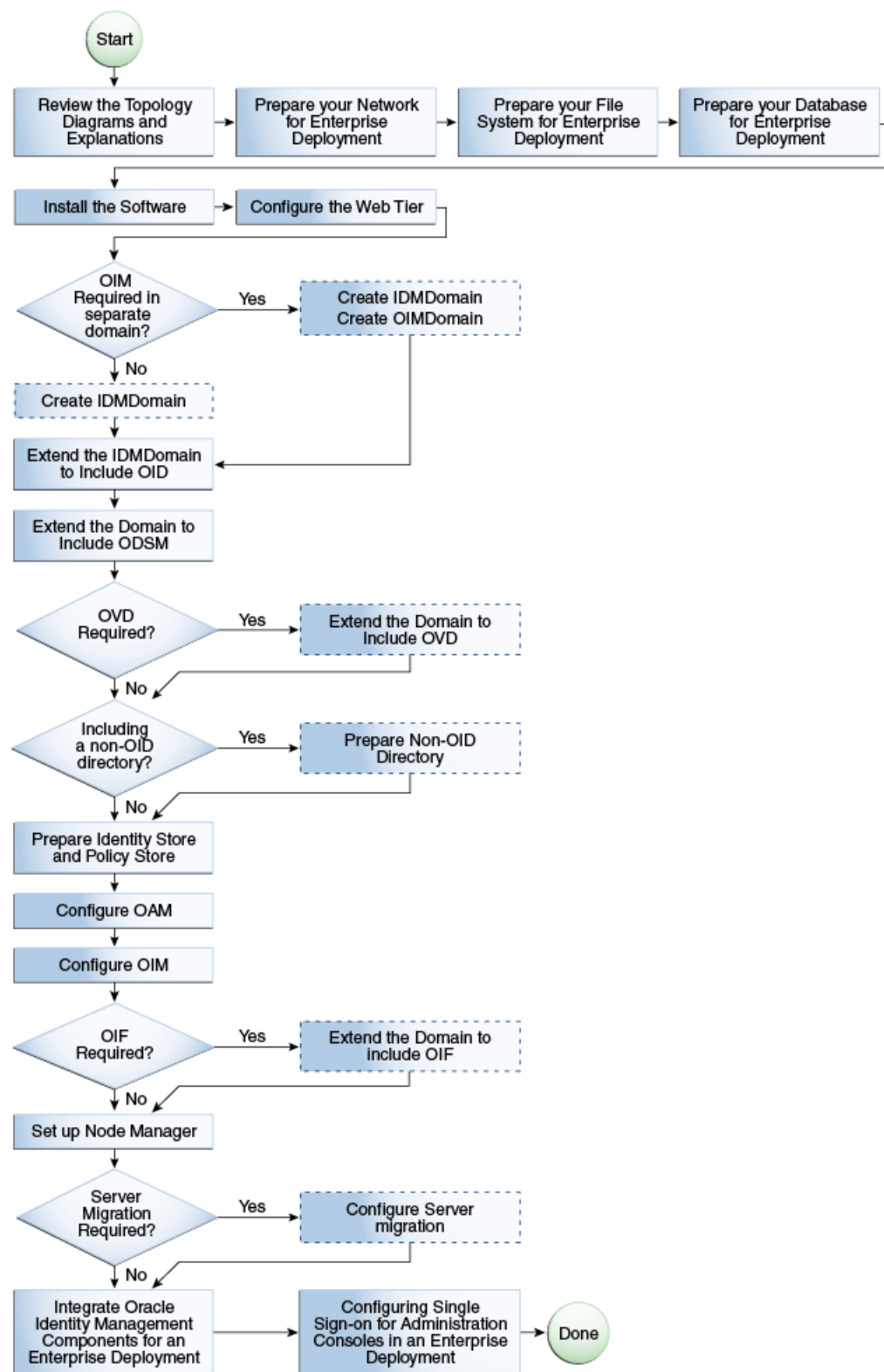
This section covers the following topics:

- [Section 2.4.1, "Flow Chart of the Oracle Identity Management Enterprise Deployment Process for Oracle Fusion Applications"](#)
- [Section 2.4.2, "Steps in the Oracle Identity Management Enterprise Deployment Process"](#)

2.4.1 Flow Chart of the Oracle Identity Management Enterprise Deployment Process for Oracle Fusion Applications

Figure 2–4, "Flow Chart of the Oracle Identity Management Enterprise Deployment Process for Oracle Fusion Applications" provides a flow chart of the Oracle Identity Management enterprise deployment process. Review this chart to become familiar with the steps that you must follow, based on the existing environment.

Figure 2-4 Flow Chart of the Oracle Identity Management Enterprise Deployment Process for Oracle Fusion Applications



2.4.2 Steps in the Oracle Identity Management Enterprise Deployment Process

Table 2–3 describes each of the steps in the enterprise deployment process flow chart for Oracle Identity Management, shown in Figure 2–4. The table also provides information on where to obtain more information about each step in the process.

Table 2–3 Steps in the Oracle Identity Management Enterprise Deployment Process

Step	Description	More Information
Prepare your Network for Enterprise Deployment	To prepare your network for an enterprise deployment, understand concepts, such as virtual server names and IPs and virtual IPs, and configure your load balancer by defining virtual host names.	Chapter 3, "Preparing the Network for an Enterprise Deployment"
Prepare your File System for Enterprise Deployment	To prepare your file system for an enterprise deployment, review the terminology for directories and directory environment variables, and configure shared storage.	Chapter 4, "Preparing the File System for an Enterprise Deployment"
Prepare your Database for Enterprise Deployment	To prepare your database for an enterprise deployment, review database requirements, create database services, load the metadata repository, in the Oracle RAC database, configure Identity Management schemas for transactional recovery privileges, and back up the database.	Chapter 5, "Preparing the Database for an Enterprise Deployment"
Install the Software	Install Oracle HTTP Server, Oracle WebLogic Server, Oracle Fusion Middleware, and apply patchsets to Oracle Fusion Middleware components.	Chapter 6, "Installing the Software for an Enterprise Deployment"
Configure the Web Tier	Configure the Oracle Web Tier by associating the Oracle Web tier with the Oracle WebLogic Domain, Configuring Oracle HTTP Server with the load balancer, and configuring virtual host names.	Chapter 7, "Configuring the Web Tier for an Enterprise Deployment"
Create a Domain	Run the Configuration Wizard to create the domains (IDMDomain and optionally OIMDomain) and include OAM and OIM.	Chapter 8, "Creating Domains for an Enterprise Deployment"
Extend the Domain for Oracle Internet Directory	Extend the existing WebLogic domain by running the Configuration Wizard to configure Oracle Internet Directory.	Chapter 9, "Extending the Domain to Include Oracle Internet Directory"
Extend the Domain for Oracle Directory Services Manager	Extend the existing WebLogic domain by running the Configuration Wizard to configure ODSM.	Chapter 10, "Extending the Domain to Include ODSM"
Prepare Identity and Policy Stores	Prepare the Identity and Policy Stores in an Oracle Identity Management enterprise deployment.	Chapter 11, "Preparing Identity and Policy Stores"

Table 2–3 (Cont.) Steps in the Oracle Identity Management Enterprise Deployment Process

Step	Description	More Information
Extend the Domain for Oracle Virtual Directory?	Extend the existing WebLogic domain by running the Configuration Wizard to configure Oracle Virtual Directory.	Chapter 12, "Extending the Domain to Include Oracle Virtual Directory"
Configure Oracle Access Manager 11g	Configure Oracle Access Manager 11g	Chapter 13, "Configuring Oracle Access Manager 11g"
Configure Oracle Identity Manager 11g	Configure Oracle Identity Manager 11g	Chapter 14, "Configuring Oracle Identity Manager"
Extend the Domain for Oracle Identity Federation?	Run the Configuration Wizard again and extend the domain to include Oracle Identity Federation.	Chapter 15, "Extending the Domain to Include Oracle Identity Federation"
Set up Node Manager	Set up Node manager by enabling host name verification, starting Node Manager, and configuring WebLogic Servers to use custom keystores.	Chapter 16, "Setting Up Node Manager for an Enterprise Deployment"
Configure Server Migration	Configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers. The WLS_OIM1 and WLS_SOA1 Managed Server are configured to restart on OIMHOST2 should a failure occur. The WLS_OIM2 and WLS_SOA2 Managed Servers are configured to restart on OIMHOST1 should a failure occur.	Chapter 17, "Configuring Server Migration for an Enterprise Deployment"
Integrate Identity Management Components	Integrate Oracle Identity Management components for an enterprise deployment.	Chapter 18, "Integrating Oracle Identity Management Components for an Enterprise Deployment"
Configure single sign-on for administration Consoles in an Enterprise Deployment	Configure single sign-on (SSO) for administration consoles in an Identity Management Enterprise deployment.	Chapter 19, "Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment"

Preparing the Network for an Enterprise Deployment

This chapter describes the prerequisites for the Oracle Identity Management Infrastructure enterprise deployment topologies.

This chapter includes the following topics:

- [Section 3.1, "Overview of Preparing the Network for an Enterprise Deployment"](#)
- [Section 3.2, "About Virtual Server Names Used by the Topologies"](#)
- [Section 3.3, "Configuring the Load Balancers"](#)
- [Section 3.4, "Load Balancer Configuration"](#)
- [Section 3.5, "About IP Addresses and Virtual IP Addresses"](#)
- [Section 3.6, "About Firewalls and Ports"](#)
- [Section 3.7, "Managing Oracle Access Manager Communication Protocol"](#)
- [Section 3.8, "About WebLogic Domains"](#)

3.1 Overview of Preparing the Network for an Enterprise Deployment

You must configure several virtual servers and associated ports on the load balancer for different types of network traffic and monitoring. These virtual servers should be configured to the appropriate real hosts and ports for the services running. Also, the load balancer should be configured to monitor the real host and ports for availability so that the traffic to these is stopped as soon as possible when a service is down. This ensures that incoming traffic on a given virtual host is not directed to an unavailable service in the other tiers.

3.2 About Virtual Server Names Used by the Topologies

The Identity Management enterprise topologies use the following virtual server names:

- [oididstore.mycompany.com](#)
- [policystore.mycompany.com](#)
- [idstore.mycompany.com](#)
- [admin.mycompany.com](#)
- [oimadmin.mycompany.com](#) (split domain topology only)
- [idminternal.mycompany.com](#)

- [sso.mycompany.com](#)

Some of the virtual server names are used by some topologies and not others.

Ensure that the virtual server names are associated with IP addresses and are part of your DNS. The computers on which Oracle Fusion Middleware is running must be able to resolve these virtual server names.

You will define the virtual server names on the load balancer using the procedure in [Section 3.3, "Configuring the Load Balancers"](#)

The rest of this document assumes that the deployment is one of those shown in [Section 2.1.1, "Reference Topologies Documented in the Guide."](#)

3.2.1 oididstore.mycompany.com

- This entry is only required if Identity information is stored in an Oracle Internet Directory and Oracle Virtual Directory is being used.
- This virtual server is enabled on LBR2. It acts as the access point for all identity-based LDAP traffic, which is stored in the Oracle Internet Directory servers in the directory tier. Traffic to both SSL and non-SSL is configured. The clients access this service using the address `oididstore.mycompany.com:3131` for SSL and `oididstore.mycompany.com:3060` for non-SSL.
- This virtual server directs traffic received on port 3060 to each of the Oracle Internet Directory instances on port 3060.
- This virtual server directs traffic received on port 3131 to each of the Oracle Internet Directory instances on port 3131.
- Monitor the heartbeat of the Oracle Internet Directory processes on LDAPHOST1 and LDAPHOST2. If an Oracle Internet Directory process stops on LDAPHOST1 or LDAPHOST2, or if either host LDAPHOST1 or LDAPHOST2 is down, the load balancer must continue to route the LDAP traffic to the surviving computer.

3.2.2 polycystore.mycompany.com

- This virtual server is enabled on LBR2. It acts as the access point for all policy-based LDAP traffic, which is stored in the Oracle Internet Directory servers in the directory tier. Traffic to both the SSL and non-SSL is configured. The clients access this service using the address `polycystore.mycompany.com:636` for SSL and `polycystore.mycompany.com:389` for non-SSL.

Note: Oracle recommends that you configure the same port for SSL connections on the LDAP server and Oracle Internet Directory on the computers on which Oracle Internet Directory is installed.

This is a requirement for most Oracle 11g products that use Oracle Internet Directory through the load balancing router.

- This virtual server directs traffic received on port 389 to each of the Oracle Internet Directory instances on port 3060.
- This virtual server directs traffic received on port 636 to each of the Oracle Internet Directory instances on port 3131.
- Monitor the heartbeat of the Oracle Internet Directory processes on LDAPHOST1 and LDAPHOST2. If an Oracle Internet Directory process stops on LDAPHOST1

or LDAPHOST2, or if either host LDAPHOST1 or LDAPHOST2 is down, the load balancer must continue to route the LDAP traffic to the surviving computer.

3.2.3 idstore.mycompany.com

- This virtual server is enabled on LBR2. It acts as the access point for all Identity Store LDAP traffic. Traffic to both the SSL and non-SSL is configured. The clients access this service using the address `idstore.mycompany.com:636` for SSL and `idstore.mycompany.com:389` for non-SSL.
- If your Identity Store is accessed through Oracle Virtual Directory, monitor the heartbeat of the Oracle Virtual Directory processes on LDAPHOST1 and LDAPHOST2. If an Oracle Virtual Directory process stops on LDAPHOST1 or LDAPHOST2, or if either host LDAPHOST1 or LDAPHOST2 is down, the load balancer must continue to route the LDAP traffic to the surviving computer.
- If your Identity Store is in Oracle Internet Directory and is accessed directly, monitor the heartbeat of the Oracle Internet Directory processes on the Oracle Internet Directory Hosts. If an Oracle Internet Directory process stops on one LDAPHOST or one LDAPHOST is down, the load balancer must continue to route the LDAP traffic to the surviving computer.
- If you have an Oracle Internet Directory-only topology, `idstore.mycompany.com` points to the Oracle Internet Directory in which you are storing your identity data. If you are storing your identity data in a third-party directory or want to front your Oracle Internet Directory Identity Store with Oracle Virtual Directory, then `idstore` points to Oracle Virtual Directory.
- If your identity store is in Oracle Internet Directory, this virtual server directs traffic received on port 389 to each of the Oracle Internet Directory instances on port 3060.
- If your identity store is in Oracle Internet Directory, this virtual server directs traffic received on port 636 to each of the Oracle Internet Directory instances on port 3131.
- If your identity store is in Oracle Virtual Directory, this virtual server directs traffic received on port 389 to each of the Oracle Virtual Directory instances on port 6501.
- If your identity store is in Oracle Virtual Directory, this virtual server directs traffic received on port 636 to each of the Oracle Virtual Directory instances on port 7501.

3.2.4 admin.mycompany.com

- This virtual server is enabled on LBR1. It acts as the access point for all internal HTTP traffic that gets directed to the administration services. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `admin.mycompany.com:80` and in turn forward these to ports 7777 on WEBHOST1 and WEBHOST2. The services accessed on this virtual host include the WebLogic Administration Server Console, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Directory Services Manager.
- Create rules in the firewall to block outside traffic from accessing the `/console` and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `admin.mycompany.com` virtual host.

3.2.5 oimadmin.mycompany.com

- This virtual server is only required if a split domain topology is being used.
- This virtual server is enabled on LBR1. It acts as the access point for all internal HTTP traffic that gets directed to the administration services in the OIM Domain. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `oimadmin.mycompany.com:80` and in turn forward these to ports 7777 on WEBHOST1 and WEBHOST2. The services accessed on this virtual host include the WebLogic Administration Server Console, Oracle Enterprise Manager Fusion Middleware Control, and Oracle Directory Services Manager for Oracle Internet Directory.
- Create rules in the firewall to block outside traffic from accessing the `/console` and `/em` URLs using this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `oimadmin.mycompany.com` virtual host.

3.2.6 idminternal.mycompany.com

- This virtual server is enabled on LBR1. The incoming traffic from clients is non-SSL enabled. Thus, the clients access this service using the address `idminternal.mycompany.com:80` and in turn forward these to ports 7777 on WEBHOST1 and WEBHOST2. The SOA Managed servers access this virtual host to callback Oracle Identity Manager web services
- Create rules in the firewall to block outside traffic from accessing this virtual host. Only traffic inside the DMZ should be able to access these URLs on the `idminternal.mycompany.com` virtual host.

3.2.7 sso.mycompany.com

- This is the virtual name which fronts all Identity Management components, including Oracle Identity Federation, Oracle Access Manager, and Oracle Identity Manager.
- This virtual server is enabled on LBR1. It acts as the access point for all HTTP traffic that gets directed to the single sign on services. The incoming traffic from clients is SSL enabled. Thus, the clients access this service using the address `sso.mycompany.com:443` and in turn forward these to ports 7777 on WEBHOST1 and WEBHOST2. All the single sign on enabled protected resources are accessed on this virtual host.
- Configure this virtual server in the load balancer with both port 80 and port 443.
- This virtual host must be configured to preserve the client IP address for a request. In some load balancers, you configure this by enabling the load balancer to insert the original client IP address of a request in an X-Forwarded-For HTTP header.

3.3 Configuring the Load Balancers

Several virtual servers and associated ports must be configured on the load balancer for different types of network traffic and monitoring. These should be configured to the appropriate real hosts and ports for the services running. Also, the load balancer should be configured to monitor the real host and ports for availability so that the traffic to these is stopped as soon as possible when a service is down. This ensures that incoming traffic on a given virtual host is not directed to an unavailable service in the other tiers.

There are two load balancer devices in the recommended topologies. One load balancer is set up for external HTTP traffic and the other load balancer is set up for internal LDAP traffic. A deployment may choose to have a single load balancer device due to a variety of reasons. While this is supported, the deployment should consider the security implications of doing this and if found appropriate, open up the relevant firewall ports to allow traffic across the various DMZs. It is worth noting that in either case, it is highly recommended to deploy a given load balancer device in fault tolerant mode.

3.3.1 Load Balancer Requirements

The enterprise topologies use an external load balancer. This external load balancer must have the following features:

- Ability to load-balance traffic to a pool of real servers through a virtual host name: Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load balance requests to the servers in the pool.
- Port translation configuration.
- Monitoring of ports (HTTP and HTTPS).
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:
 - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle WebLogic Clusters, the load balancer must be configured with a virtual server and ports for HTTP and HTTPS traffic.
 - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.
- Ability to detect node failures and immediately stop routing traffic to the failed node.
- Resource monitoring / port monitoring / process failure detection: The load balancer must be able to detect service and node failures (through notification or some other means) and to stop directing non-Oracle Net traffic to the failed node. If your external load balancer has the ability to automatically detect failures, you should use it.
- Fault tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- Other: It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the back-end services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.
- SSL acceleration (this feature is recommended, but not required).
- Configure the virtual server(s) in the load balancer for the directory tier with a high value for the connection timeout for TCP connections. This value should be more than the maximum expected time over which no traffic is expected between Oracle Access Manager and the directory tier.

- **Ability to Preserve the Client IP Addresses:** The Load Balancer must have the capability to insert the original client IP address of a request in an X-Forwarded-For HTTP header to preserve the Client IP Address.

3.3.2 Load Balancer Configuration Procedures

The procedures for configuring a load balancer differ, depending on the specific type of load balancer. Refer to the vendor supplied documentation for actual steps. The following steps outline the general configuration flow:

1. Create a pool of servers. This pool contains a list of servers and the ports that are included in the load balancing definition. For example, for load balancing between the web hosts you create a pool of servers which would direct requests to hosts WEBHOST1 and WEBHOST2 on port 7777.
2. Create rules to determine whether or not a given host and service is available and assign it to the pool of servers described in Step 1.
3. Create a Virtual Server on the load balancer. This is the address and port that receives requests used by the application. For example, to load balance Web Tier requests you would create a virtual host for `sso.mycompany.com:80`.
4. If your load balancer supports it, specify whether or not the virtual server is available internally, externally or both. Ensure that internal addresses are only resolvable from inside the network.
5. Configure SSL Termination, if applicable, for the virtual server.
6. Assign the Pool of servers created in Step 1 to the virtual server.
7. Tune the time out settings as listed in [Table 0–3, "Ports Used in the Oracle Identity Management Enterprise Deployment topologies"](#). This includes time to detect whether a service is down.

3.4 Load Balancer Configuration

For an Identity Management deployment, configure your load balancer as shown in [Table 3–1](#).

Table 3–1 Load Balancer Configuration

Virtual Host	Server Pool	Protocol	SSL Termination	External	Other Required Configuration/Comments
sso.mycompany.com:80	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTP	No	Yes	Identity Management requires that the following be added to the HTTP header: Header Name: IS_SSL ¹ Header Value: ssl

Table 3–1 (Cont.) Load Balancer Configuration

Virtual Host	Server Pool	Protocol	SSL Termination	External	Other Required Configuration/Comments
sso.mycompany.com:443	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTPS	Yes	Yes	Identity Management requires that the following be added to the HTTP header: Header Name: IS_SSL Header Value: ssl
idinternal.mycompany.com:80	WEBHOST1/2:7777	HTTP	No	No	
admin.mycompany.com:80	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTP	No	No	
oimadmin.mycompany.com:80	WEBHOST1.mycompany.com:7777 WEBHOST2.mycompany.com:7777	HTTP	No	No	Split Domain Topology Only
polycstore.mycompany.com:389	LDAPHOST1.mycompany.com:3060 LDAPHOST2.mycompany.com:3060	LDAP	No	No	
polycstore.mycompany.com:636	LDAPHOST1.mycompany.com:3131 LDAPHOST2.mycompany.com:3131	LDAP	No	No	
idstore.mycompany.com:389	LDAPHOST1.mycompany.com:6501 LDAPHOST2.mycompany.com:6501	LDAP	No	No	If you have an Oracle Internet Directory-only topology and are not using Oracle Virtual Directory, the server pool must contain Oracle Internet Directory servers.

Table 3–1 (Cont.) Load Balancer Configuration

Virtual Host	Server Pool	Protocol	SSL Termination	External	Other Required Configuration/Comments
idstore.mycompany.com:636	LDAPHOST1.mycompany.com:7501 LDAPHOST2.mycompany.com:7501	LDAP	No	No	If you have an Oracle Internet Directory-only topology and are not using Oracle Virtual Directory, the server pool must contain Oracle Internet Directory servers.
oididstore.mycompany.com:3060	LDAPHOST1.mycompany.com:3060 LDAPHOST2.mycompany.com:3060	LDAP	No	No	Only required if Identity Management users are stored in an Oracle Internet Directory and Oracle Virtual Directory is being used.
oididstore.mycompany.com:3131	LDAPHOST1.mycompany.com:3131 LDAPHOST2.mycompany.com:3131	LDAP	No	No	Only required if Identity Management users are stored in an Oracle Internet Directory and Oracle Virtual Directory is being used.

¹ For information about configuring IS_SSL, see "About User Defined WebGate Parameters" in *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

3.5 About IP Addresses and Virtual IP Addresses

A virtual IP address is an unused IP Address which belongs to the same subnet as the host's primary IP address. It is assigned to a host manually and Oracle WebLogic Managed servers are configured to listen on this IP Address. In the event of the failure of the node where the IP address is assigned, the IP address is assigned to another node in the same subnet, so that the new node can take responsibility for running the managed servers assigned to it.

The following is a list of the Virtual IP addresses required by Oracle Identity Management:

- adminvhn.mycompany.com

In Enterprise deployments the WebLogic Administration Server must be able to continue processing requests after the host it is residing on fails. A virtual IP address should be provisioned in the application tier so that it can be bound to a

network interface on any host in the application tier. The WebLogic Administration Server is configured later to listen on this virtual IP address, as discussed later in this manual. The virtual IP address fails over along with the Administration Server from IDMHOST1 to IDMHOST2, or vice versa.

- oimadminvhn.mycompany.com

You need this virtual IP address if you are using a split domain topology. It serves a similar function to adminvhn.mycompany.com. This virtual IP address fails over along with the Administration Server from OIMHOST1 to OIMHOST2, or vice versa.

- soahostxvhn.mycompany.com

One virtual IP address is required for each SOA managed server. This enables the servers to participate in Server migration.

Provision a virtual IP address in the application tier so that it can be bound to a network interface on any host in the application tier.

- oimhostxvhn.mycompany.com

One virtual IP Address is required for each Oracle Identity Manager managed server. This enables the servers to participate in Server migration.

Provision a virtual IP address in the application tier so that it can be bound to a network interface on any host in the application tier.

Configure the Administration Server and the managed servers to listen on different virtual IPs and physical IPs as illustrated in [Figure 3–1](#). For a split domain topology, configure them as illustrated in [Figure 3–2](#).

Figure 3–1 IPs and VIPs Mapped to Administration Server and Managed Servers

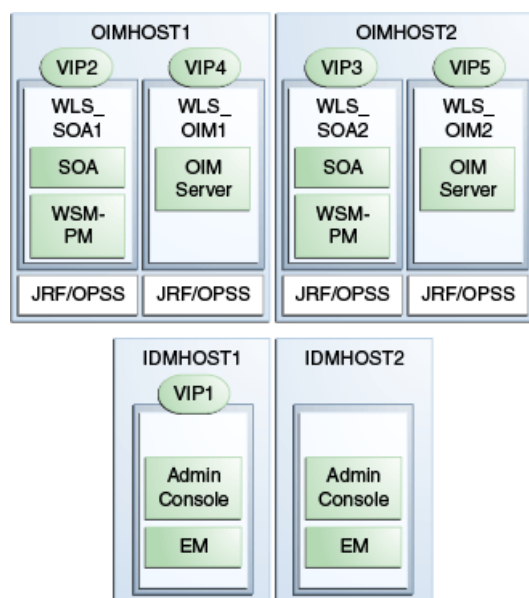


Figure 3–2 IPs and VIPs Mapped to Administration Server and Managed Servers: Split Domain Topology

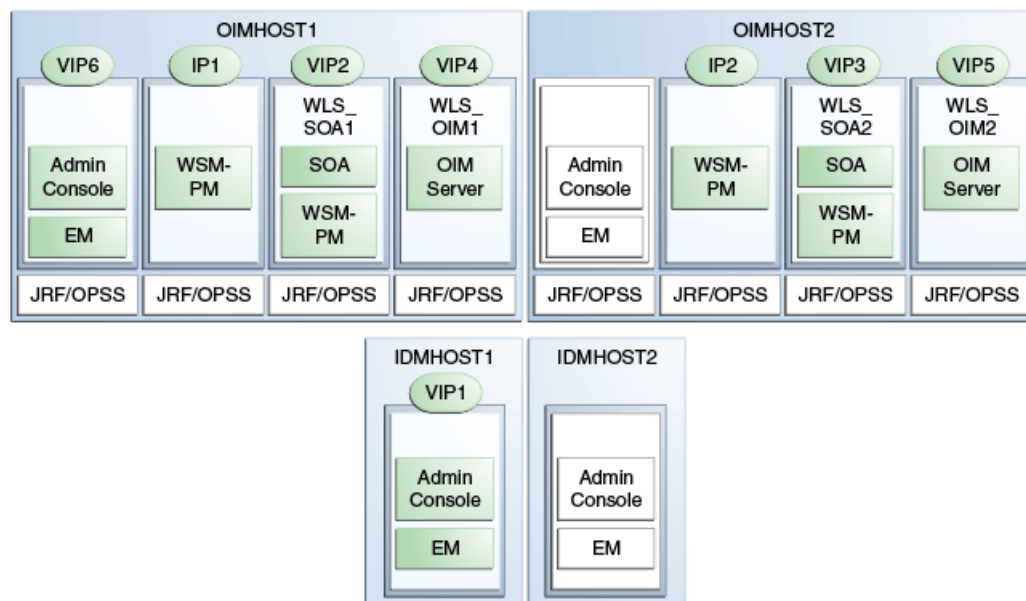


Table 3–2 provides descriptions of the various virtual hosts.

Table 3–2 Virtual Hosts

Virtual IP	VIP Maps to...	Description
VIP1	ADMINVHN	ADMINVHN is the virtual host name that is the listen address for the Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running (IDMHOST1 by default).
VIP2	SOAHOST1VHN	SOAHOST1VHN is the virtual host name that maps to the listen address for WLS_SOA1 and fails over with server migration of this managed server. It is enabled on the node where WLS_SOA1 process is running (OIMHOST1 by default).
VIP3	SOAHOST2VHN	SOAHOST2VHN is the virtual host name that maps to the listen address for WLS_SOA2 and fails over with server migration of this managed server. It is enabled on the node where WLS_SOA2 process is running (OIMHOST2 by default).
VIP4	OIMHOST1VHN	OIMHOST1VHN is the virtual host name that maps to the listen address for the WLS_OIM1 server and fails over with server migration of this server. It is enabled in the node where the WLS_OIM1 process is running (OIMHOST1 by default).
VIP5	OIMHOST2VHN	OIMHOST2VHN is the virtual host name that maps to the listen address for the WLS_OIM2 server and fails over with server migration of this server. It is enabled in the node where the WLS_OIM2 process is running (OIMHOST2 by default).

Table 3–2 (Cont.) Virtual Hosts

Virtual IP	VIP Maps to...	Description
VIP6	OIMADMINVHN	OIMADMINVHN is the virtual host name that is the listen address for the Oracle Identity Manager Administration Server. It fails over with manual failover of the Administration Server. It is enabled on the node where the Oracle Identity Manager Administration Server process is running (OIMHOST1 by default).

3.6 About Firewalls and Ports

Many Oracle Fusion Middleware components and services use ports. As an administrator, you must know the port numbers used by these services, and to ensure that the same port number is not used by two services on a host.

Most port numbers are assigned after installation. You can use different port numbers if you want to. The port numbers shown in [Table 3–3](#) are examples that are used throughout this guide for consistency. If you use different port numbers, you must substitute those values for the values in the table wherever they are used.

[Table 3–3](#) lists the ports used in the Oracle Identity Management topologies, including the ports that you must open on the firewalls in the topologies.

Firewall notation:

- FW0 refers to the outermost firewall.
- FW1 refers to the firewall between the web tier and the application tier.
- FW2 refers to the firewall between the application tier and the directory tier.

Table 3–3 Ports Used in the Oracle Identity Management Enterprise Deployment topologies

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Browser request	FW0	80	HTTP / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity Management.
Browser request	FW0	443	HTTPS / Load balancer	Both	Timeout depends on all HTML content and the type of process model used for Oracle Identity Management.
Browser request	FW1	80	HTTP / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for IDM.
Browser request	FW1	443	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for IDM.

Table 3–3 (Cont.) Ports Used in the Oracle Identity Management Enterprise Deployment topologies

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
Load balancer to Oracle HTTP Server	n/a	7777	HTTP	n/a	See Section 3.3, "Configuring the Load Balancers."
OHS registration with Administration Server	FW1	7001	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
IDMDomain Oracle WebLogic Administration Server access from web tier	FW1	7001	HTTP / Oracle HTTP Server and Administration Server	Inbound	N/A
Enterprise Manager Agent - web tier to Enterprise Manager	FW1	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A
Oracle HTTP Server to WLS_ODS	FW1	7006	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the mod_weblogic parameters used.
Oracle HTTP Server to WLS_OAM	FW1	14100	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the mod_weblogic parameters used.
Oracle HTTP Server WLS_OIM	FW1	14000	HTTP / Oracle HTTP Server to WebLogic Server	Inbound	Timeout depends on the mod_weblogic parameters used
Oracle HTTP Server WLS_SOA	FW1	8001	HTTP / Oracle HTTP Server to WebLogic Server	Both	Timeout depends on the mod_weblogic parameters used
Oracle HTTP Server management by Administration Server	FW1	OPMN remote port (6701) and OHS Admin Port (7779)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period, such as 5-10 seconds.
Oracle Access Manager Server 11g	FW1	5574-5575	OAP	Both	N/A
Oracle Access Manager Coherence port	FW1	9095	TCMP	Both	N/A
Oracle Coherence Port	FW1	8000 - 8088	TCMP	Both	N/A
IDMDomain Oracle WebLogic Administration Server access from directory tier	FW2	7001	HTTP / Oracle Internet Directory, Oracle Virtual Directory, and Administration Server	Outbound	N/A
OIMDomain Oracle WebLogic Administration Server access from directory tier	FW2	7001	HTTP / Oracle Internet Directory, Oracle Virtual Directory, and Administration Server	Outbound	N/A
Enterprise Manager Agent - directory tier to Enterprise Manager	FW2	5160	HTTP / Enterprise Manager Agent and Enterprise Manager	Both	N/A

Table 3–3 (Cont.) Ports Used in the Oracle Identity Management Enterprise Deployment topologies

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Timeout
OPMN access in directory tier	FW2	OPMN remote port	HTTP / Administration Server to OPMN	Inbound	N/A
Oracle Virtual Directory proxy port	FW2	8899	HTTP / Administration Server to Oracle Virtual Directory	Inbound	N/A
Database access	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle Identity Management.
Oracle Internet Directory access	FW2	3060	LDAP	Inbound	Tune the directory server's parameters based on the load balancer, and not the other way around. Ideally, these connections should be configured not to time out.
Oracle Internet Directory access	FW2	3131	LDAP SSL	Inbound	Tune the directory server's parameters based on the load balancer, and not the other way around. Ideally, these connections should be configured not to time out.
Oracle Virtual Directory access	FW2	6501	LDAP	Inbound	Ideally, these connections should be configured not to time out.
Oracle Virtual Directory access	FW2	7501	LDAP SSL	Inbound	Ideally, these connections should be configured not to time out.
Oracle Identity Federation	FW2	7499	HTTP	Both	N/A
Oracle Identity Navigator	FW2	7001	HTTP	Both	N/A
Load balancer to Oracle HTTP Server	N/A	7777	HTTP	N/A	N/A
Session replication within a WebLogic Server cluster	N/A	N/A	N/A	N/A	By default, this communication uses the same port as the server's listen address.
Node Manager	N/A	5556	TCP/IP	N/A	N/A

Note: Additional ports might need to be opened across the firewalls to enable applications in external domains, such as SOA or WebCenter Portal domains, to authenticate against this Identity Management domain.

3.7 Managing Oracle Access Manager Communication Protocol

This section discusses Oracle Access Protocol (OAP) and provides an overview of a user request.

3.7.1 Oracle Access Manager Protocols

Oracle Access Protocol (OAP) enables communication between Access System components (for example, OAM Server, WebGate) during user authentication and authorization. This protocol was formerly known as NetPoint Access Protocol (NAP) or COREid Access Protocol.

3.7.2 Overview of Integration Requests

Oracle Access Manager is responsible for creating sessions for users. When Oracle Access Manager is integrated with another Identity Management component, such as Oracle Identity Manager, authentication is delegated to those components.

A typical request flow is as follows:

1. The user tries to access a resource for the first time.
2. WebGate intercepts the request and detects that the user is not authenticated.
3. Oracle Access Manager credential collector is invoked and the user enters a user name and password in response to a prompt. Oracle Access Manager knows that password policy requires the password to be changed at first login, so the user's browser is redirected to Oracle Identity Manager.
4. The user is prompted to change password and set up challenge questions.
5. At this point, Oracle Identity Manager has authenticated the user using the newly entered password. Oracle Identity Manager creates a TAP request to say that Oracle Access Manager can create a session for the user. That is, the user will not be expected to log in again. This is achieved by adding a token to the user's browser that Oracle Access Manager can read.

The TAP request to Oracle Access Manager will include such things as:

- Where the Oracle Access Manager servers are located.
- What web gate profile to use.
- WebGate profile password.
- Certificates, if Oracle Access Manager is working in simple or cert mode.

3.7.3 Overview of User Request

The request flow when a user requests access is as follows:

1. The user requests access to a protected resource over HTTP or HTTPS.
2. The WebGate intercepts the request.

3. The WebGate forwards the request to the OAM Server over Oracle Access Protocol to determine if the resource is protected, how, and whether the user is authenticated (if not, there is a challenge).
4. The OAM Server checks the directory server for credentials such as a user ID and password, sends the information back to WebGate over Oracle Access Protocol, and generates an encrypted cookie to authenticate the user.
5. Following authentication, the WebGate prompts the OAM Server over Oracle Access Protocol and the OAM Server looks up the appropriate security policies, compares them to the user's identity, and determines the user's level of authorization.
 - If the access policy is valid, the user is allowed to access the desired content and/or applications.
 - If the policy is false, the user is denied access and redirected to another URL determined by the organization's administrator.

3.8 About WebLogic Domains

A domain is the basic administration unit for WebLogic Server instances. A domain consists of one or more WebLogic Server instances (and their associated resources) that you manage with a single Administration Server. You can define multiple domains based on different system administrators' responsibilities, application boundaries, or geographical locations of servers. Conversely, you can use a single domain to centralize all WebLogic Server administration activities.

In the context of Identity Management, it is recommended that you deploy the Identity Management components, plus SOA, in a separate WebLogic Server domain from the one where SOA, WebCenter Portal and other customer applications might be deployed. In a typical enterprise deployment, the administration of identity management components such as LDAP directory, single sign-on solutions, and provisioning solutions is done by a different set of administrators from those who administer the middleware infrastructure and applications. Oracle Identity Manager can be deployed into a separate dedicated domain so that it can be patched independently of other products.

It is technically possible to deploy everything in a single domain in a development or test environment. However, in a production environment, the recommendation to use separate domains creates a logical administrative boundary between the identity management stack and the rest of the middleware and application deployment.

Preparing the File System for an Enterprise Deployment

This chapter describes how to prepare the file system for an Oracle Identity Management enterprise deployment.

The file system model described in this guide was chosen for maximum availability, best isolation of components, symmetry in the configuration, and facilitation of backup and disaster recovery. The rest of the guide uses this directory structure and directory terminology. Other directory layouts are possible and supported.

This chapter contains the following topics:

- [Section 4.1, "Overview of Preparing the File System for Enterprise Deployment"](#)
- [Section 4.2, "Terminology for Directories and Directory Variables"](#)
- [Section 4.3, "ASERVER_HOME and MSERVER_HOME"](#)
- [Section 4.4, "About Recommended Locations for the Different Directories"](#)
- [Section 4.5, "Configuring Shared Storage"](#)

4.1 Overview of Preparing the File System for Enterprise Deployment

It is important to set up your file system in a way that makes the enterprise deployment easier to understand, configure, and manage. Oracle recommends setting up your file system according to information in this chapter. The terminology defined in this chapter is used in diagrams and procedures throughout the guide.

Use this chapter as a reference to help understand the directory variables used in the installation and configuration procedures. Other directory layouts are possible and supported, but the model adopted in this guide is chosen for maximum availability, providing both the best isolation of components and symmetry in the configuration and facilitating backup and disaster recovery. The rest of the document uses this directory structure and directory terminology.

4.2 Terminology for Directories and Directory Variables

This section describes the directory variables used throughout this guide for configuring the Oracle Identity Management enterprise deployment. You are not required to set these as environment variables. The following directory variables are used to describe the directories installed and configured in the guide:

- **ORACLE_BASE**: This environment variable and related directory path refers to the base directory under which Oracle products are installed. For example:
u01/app/oracle

- **MW_HOME:** This variable and related directory path refers to the location where Oracle Fusion Middleware resides. A *MW_HOME* has a *WL_HOME*, an *ORACLE_COMMON_HOME* and one or more *ORACLE_HOMES*. An example of a typical *MW_HOME* is:

ORACLE_BASE/product/fmw

There will be a different *MW_HOME* for each domain.

- **WL_HOME:** This variable and related directory path contains installed files necessary to host a WebLogic Server, for example *MW_HOME/wlserver_10.3*.
- **ORACLE_HOME:** This variable points to the location where an Oracle Fusion Middleware product, such as Oracle HTTP Server, Oracle SOA Suite, or Oracle Internet Directory is installed and the binaries of that product are being used in a current procedure. For example: *MW_HOME/iam*
- **ORACLE_COMMON_HOME:** This variable and related directory path refer to the location where the Oracle Fusion Middleware Common Java Required Files (JRF) Libraries and Oracle Fusion Middleware Enterprise Manager Libraries are installed. An example is: *MW_HOME/oracle_common*
- **Domain directory:** This path refers to the file system location where the Oracle WebLogic domain information (configuration artifacts) is stored. Different WebLogic Servers can use different domain directories even when in the same node as described [Section 4.4, "About Recommended Locations for the Different Directories."](#)
- **ORACLE_INSTANCE:** An Oracle instance contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory. An Oracle instance directory contains updatable files, such as configuration files, log files, and temporary files. An example is: *ORACLE_BASE/admin/web1*
- **ASERVER_HOME:** This is the primary location of the domain configuration. A typical example is: *ORACLE_BASE/admin/IDMDomain/aserver*
- **MSERVER_HOME:** This is a copy of the domain configuration used to start and stop managed servers. A typical example is: *ORACLE_BASE/admin/IDMDomain/mserver*
- **WEBGATE_ORACLE_HOME:** This is the location of the WebGate installation.

4.3 ASERVER_HOME and MSERVER_HOME

As described in the previous section *ASERVER_HOME* and *MSERVER_HOME* are two locations for the domain, a primary and a copy location, respectively. Having two separate locations allows you to administer the managed servers independently of the administration server.

ASERVER_HOME, the primary copy, is mounted on shared storage so that the administration server can be failed over to another host if the primary host becomes unavailable. This is necessary because the administration server is a singleton service. That is, it can only be active on one host at any given time. *ASERVER_HOME* is placed onto shared storage and is mounted exclusively to the host which is running the administration server. In the event of the failure of that host, the *ASERVER_HOME* directory is mounted on a different host and the administration server started on that host.

A copy of the domain server, *MSERVER_HOME*, is placed onto local storage, and managed servers are started from this copy. You create the copy using the weblogic utilities pack and unpack. The reason for using the copy is that starting managed servers from

shared storage is unnecessary and incurs a performance penalty. Allowing managed servers to write to local storage eliminates the performance problem.

When extending a domain, always use the primary *ASERVER_HOME* location.

4.4 About Recommended Locations for the Different Directories

Oracle Fusion Middleware 11g enables you to create multiple Identity Management components from one single binary installation. This allows you to install binaries in a single location on a shared storage and reuse this installation for the servers in different nodes.

When an *ORACLE_HOME* or a *WL_HOME* is shared by multiple servers in different nodes, keep the Oracle Inventory and Middleware home lists in those nodes updated for consistency in the installations and application of patches. To update the *oraInventory* in a node and attach an installation in a shared storage to it, use *ORACLE_HOME/oui/bin/attachHome.sh*. To update the Middleware home list to add or remove a *WL_HOME*, edit the file *beahomelist* located in a directory called *bea* in the users home directory, for example: */home/oracle/bea/beahomelist*. This is required for any nodes installed in addition to the two used in this Enterprise Deployment. An example of the *oraInventory* and *beahomelist* updates is provided in the scale-out steps included in this guide. See [Section 20.4.2, "Scaling Out the Topology."](#)

Oracle recommends also separating the domain directory used by the WebLogic Administration Server from the domain directory used by managed servers. This allows a symmetric configuration for the domain directories used by managed servers and isolates the failover of the Administration Server. The domain directory for the Administration Server must reside in shared storage to allow failover to another node with the same configuration. The managed servers' domain directories can reside in local or shared storage.

You can use a shared domain directory for all managed servers in different nodes or use one domain directory for each node. Sharing domain directories for managed servers facilitates the scale-out procedures. It is not recommended to place managed server directories onto shared storage because of the potential performance impact. In this case, the deployment should conform to the requirements (if any) of the storage system to facilitate multiple machines mounting the same shared volume. The configuration steps provided in this Enterprise Deployment Topology assume that a local domain directory for each node is used for each managed server.

All procedures that apply to multiple local domain directories apply to a single shared domain directory. Therefore, this enterprise deployment guide uses a model where one domain directory is used for each node. The directory can be local or reside in shared storage.

JMS file stores and JTA transaction logs must be placed on shared storage in order to ensure that they are available from multiple boxes for recovery in the case of a server failure or migration.

For the application tier, it is recommended to have Middleware Home (*MW_HOME*) on a shared disk. It is recommended to have two *MW_HOMES* in the domain for High Availability. An application tier node mounts either one of these on a mount point. This mount point should be the same on all the application tier nodes. Additional servers (when scaling out or up) of the same type can use one of these *MW_HOMES* without requiring more installations.

If you are implementing a split domain topology, you also need a separate *MW_HOME* for the second domain. This will facilitate independent patching.

This section contains the following topics:

- [Section 4.4.1, "Local Storage"](#)
- [Section 4.4.2, "Shared Storage"](#)
- [Section 4.4.3, "Redundant Binary Installations"](#)
- [Section 4.4.4, "Directory Structure"](#)

4.4.1 Local Storage

In an Enterprise Deployment it is recommended that the following directories be created on local storage:

Table 4–1 Local Storage Directories

Tier	Environment Variable	Directory	Hosts
Web Tier	<i>MW_HOME1</i>	<i>/u01/app/oracle/product/fmw</i>	WEBHOST1 WEBHOST2
Web Tier	<i>ORACLE_INSTANCE</i>	<i>/u01/app/oracle/admin/instancename</i>	WEBHOST1 WEBHOST2
Directory Tier	<i>ORACLE_INSTANCE</i>	<i>/u01/app/oracle/admin/instancename</i>	LDAPHOST1 LDAPHOST2
Directory Tier	<i>MW_HOME2</i>	<i>/u01/app/oracle/product/fmw</i>	LDAPHOST1 LDAPHOST2
Application Tier	<i>MSERVER_HOME</i>	<i>/u01/app/oracle/admin/domain_name/mserver</i>	IDMHOST1 IDMHOST2 OIMHOST1 OIMHOST2

While it is recommended that you put *ORACLE_INSTANCE* directories onto local storage, you can use shared storage. If you use shared storage, you must ensure that the HTTP lock file is placed on discrete locations.

4.4.2 Shared Storage

In an Enterprise Deployment, it is recommended that the volumes shown in [Table 4–2](#) or [Table 4–3](#) be created on shared Storage. Note that the details differ, depending on whether you are using a single domain or split domain topology. You can mount shared storage either exclusively or shared. If you mount it exclusively, it will be mounted to only one host at a time. (This is typically used for active/passive failover).

When scaling out or scaling up, you can use the shared *MW_HOME* for additional servers of the same type without performing more software installations.

Table 4–2 Volumes on Shared Storage, Single Domain Topology

Tier	Environment Variable	Volume	Mount Point	Mounted on Hosts	Exclusive Mount
Application Tier	<i>MW_HOME3</i>	<i>VOL1/MW_HOME3</i>	<i>/u01/app/oracle/product/fmw</i>	IDMHOST1 IDMHOST2 OIMHOST1 OIMHOST2	No

Table 4–2 (Cont.) Volumes on Shared Storage, Single Domain Topology

Tier	Environment Variable	Volume	Mount Point	Mounted on Hosts	Exclusive Mount
Application Tier	ASERVER_HOME	VOL1/ADMIN1	/u01/app/oracle/admin/IDMDomain/aserver	IDMHOST1 IDMHOST2	Yes
Application Tier		VOL1/SOA	/u01/app/oracle/admin/IDMDomain/soa_cluster	OIMHOST1 OIMHOST2	No
Application Tier		VOL1/OIM	/u01/app/oracle/admin/IDMDomain/oim_cluster	OIMHOST1 OIMHOST2	No

Table 4–3 Volumes on Shared Storage, Split Domain Topology

Tier	Environment Variable	Volume	Mount Point	Mounted on Hosts	Exclusive Mount
Application Tier	MW_HOME3	VOL1/MW_HOME3	/u01/app/oracle/product/fmw	IDMHOST1 IDMHOST2	No
Application Tier	ASERVER_HOME	VOL1/ADMIN1	/u01/app/oracle/admin/IDMDomain/aserver	IDMHOST1 IDMHOST2	Yes
Application Tier	MW_HOME4	VOL2/MW_HOME4	/u01/app/oracle/product/fmw	OIMHOST1 OIMHOST2	No
Application Tier	ASERVER_HOME	VOL2/ADMIN2	/u01/app/oracle/admin/OIMDomain/aserver	OIMHOST1 OIMHOST2	Yes
Application Tier		VOL2/SOA	/u01/app/oracle/admin/OIMDomain/soa_cluster	OIMHOST1 OIMHOST2	No
Application Tier		VOL2/OIM	/u01/app/oracle/admin/OIMDomain/oim_cluster	OIMHOST1 OIMHOST2	No

4.4.3 Redundant Binary Installations

For maximum availability, Oracle recommends using redundant binary installations. In the redundant Enterprise deployment model, you create two identical *MW_HOMEs*, each of which has a *WL_HOME* and an *ORACLE_HOME* for each product suite in shared storage. You then mount one of these *MW_HOMEs* to one set of servers, and the other to the remaining ones. Each *MW_HOME* has the same mount point, so regardless of which server you are connected to, *MW_HOME* has the same path.

Adopting this approach protects you from user errors, such as accidental deletion of files in the *MW_HOME*. Should such an error occur, only half your servers are affected. Ideally, these *MW_HOME*s should be on two different volumes in order to isolate the failures in each volume as much as possible. For additional protection, Oracle recommends that you disk mirror these volumes.

If separate volumes are not available on shared storage, Oracle recommends simulating separate volumes using different directories within the same volume and mounting these to the same mount location on the host side. Although this does not guarantee the protection that multiple volumes provide, it does allow protection from user deletions and individual file corruption.

4.4.4 Directory Structure

This section provides diagrams to help illustrate the recommended directory structure and shared storage.

[Figure 4–1](#) shows the recommended directory structure.

[Figure 4–2](#) shows the recommended structure to use with a split directory topology.

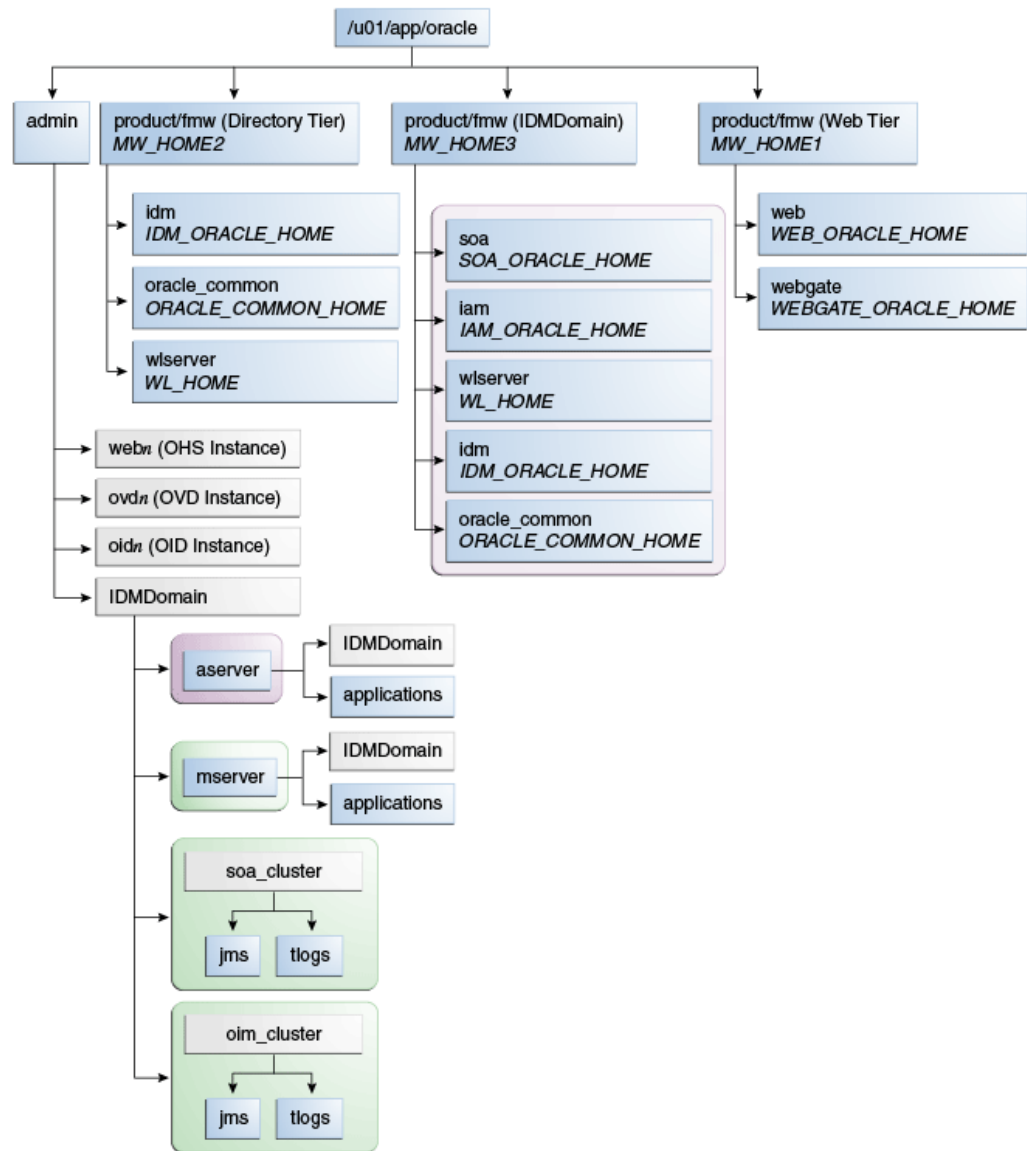
Figure 4–1 Directory Structure for Identity Management

Figure 4–2 Directory Structure for Identity Management Split Domain Topology

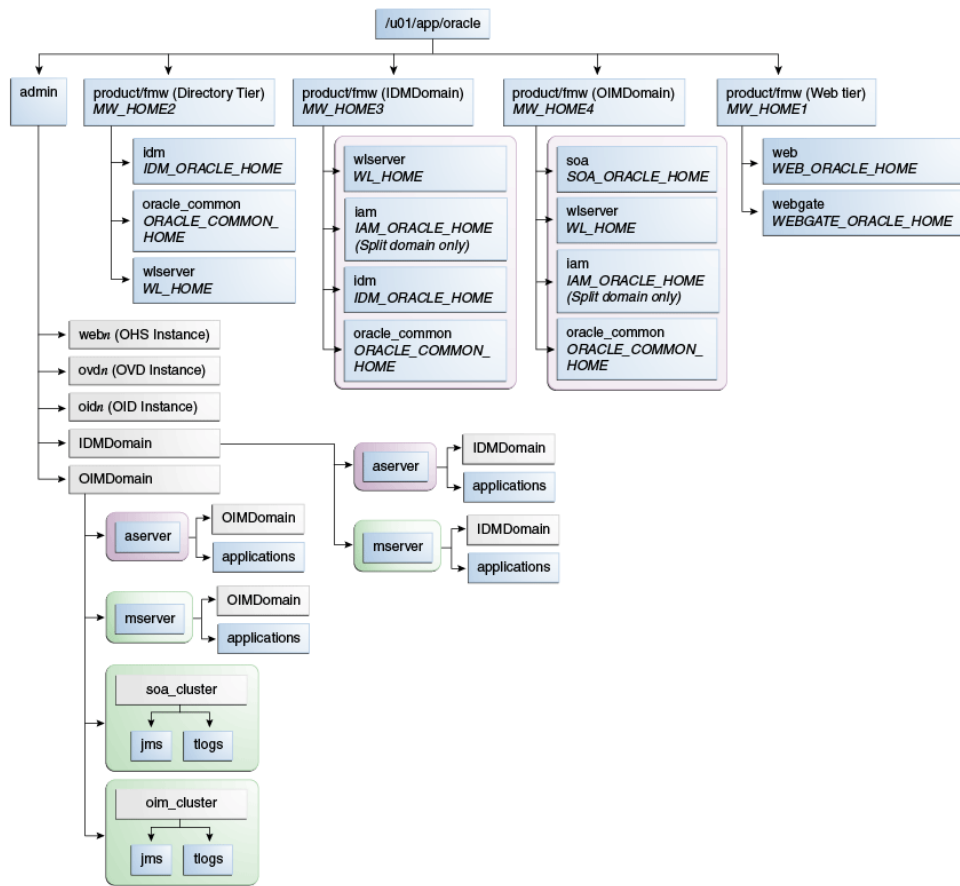






Table 4–4 explains what the color-coded elements in Figure 0–1 and Figure 0–2 mean.

Table 4–4 Directory Structure Elements

Element	Explanation
	The Administration Server domain directories, applications, deployment plans, file adapter control directory, JMS and TX logs, and the entire <i>MW_HOME</i> are on a shared disk.
	The Managed Server domain directories can be on a local disk or a shared disk. If you are using shared disk, then the directory must be exclusively mounted to a named host.
	Fixed name.
	Installation-dependent name.

4.5 Configuring Shared Storage

Use the following commands to create and mount shared storage locations so that each server pair, such as IDMHOST1 and IDMHOST2, can see the same location for binary installation in two separate volumes. Repeat the commands for the following server pairs:

1. IDMHOST1 and IDMHOST2
2. OIMHOST1 and OIMHOST2

Note: The user ID used to create a shared storage file system owns and has read, write, and execute privileges for those files. Other users in the operating system group can read and execute the files, but they do not have write privileges. For more information about installation and configuration privileges, see the "Understanding Installation and Configuration Privileges and Users" section in the *Oracle Fusion Middleware Installation Planning Guide*.

nasfiler is the shared storage filer.

From IDMHOST1:

```
mount nasfiler:/vol/vol1/ORACLE_BASE/product/fmw
ORACLE_BASE/product/fmw -t nfs
```

```
mount nasfiler:/vol/vol1/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs
/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs -t nfs
```

```
mount nasfiler:/vol/vol1/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs
/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs -t nfs
```

From IDMHOST2:

```
mount nasfiler:/vol/vol1/ORACLE_BASE/product/fmw
ORACLE_BASE/product/fmw -t nfs
```

```
mount nasfiler:/vol/vol1/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs
/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs -t nfs
```

```
mount nasfiler:/vol/vol1/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs
/ORACLE_BASE/stores/idmdomain/soa_cluster/tlogs -t nfs
```

Validating the Shared Storage Configuration

Ensure that you can read and write files to the newly mounted directories by creating a test file in the shared storage location you just configured.

For example:

```
$ cd newly mounted directory
$ touch testfile
```

Verify that the owner and permissions are correct:

```
$ ls -l testfile
```

Then remove the file:

```
$ rm testfile
```

Note: The shared storage can be a NAS or SAN device. The following illustrates an example of creating storage for a NAS device from IDMHOST1. The options may differ depending on the specific storage device.

```
mount nasfiler:/vol/vol1/fmw11shared ORACLE_BASE/wls -t nfs -o  
rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsz=32768, wsize=32768
```

Contact your storage vendor and machine administrator for the correct options for your environment.

Preparing the Database for an Enterprise Deployment

This chapter describes how to install and configure the Identity Management database repositories.

This chapter contains the following topics:

- [Section 5.1, "Overview of Preparing the Databases for an Identity Management Enterprise Deployment"](#)
- [Section 5.2, "Verifying the Database Requirements for an Enterprise Deployment"](#)
- [Section 5.3, "Installing the Database for an Enterprise Deployment"](#)
- [Section 5.4, "Creating Database Services"](#)
- [Section 5.5, "Loading the Identity Management Schemas in the Oracle RAC Database by Using RCU"](#)
- [Section 5.6, "Backing up the Database"](#)

5.1 Overview of Preparing the Databases for an Identity Management Enterprise Deployment

The Identity Management components in the enterprise deployment use database repositories. This chapter describes how to perform the following steps:

- Verify the database requirements as described in [Section 5.2, "Verifying the Database Requirements for an Enterprise Deployment."](#)
- Install and configure the Oracle database repositories. See the installation guides listed in the ["Related Documents"](#) section of the Preface and [Section 5.3, "Installing the Database for an Enterprise Deployment."](#)
- Create database services, as described in [Section 5.4, "Creating Database Services."](#)
- Create the required Oracle schemas in the database using the Repository Creation Utility (RCU). See [Section 5.5, "Loading the Identity Management Schemas in the Oracle RAC Database by Using RCU."](#)

5.2 Verifying the Database Requirements for an Enterprise Deployment

Before loading the metadata repository into your databases, check that they meet the requirements described in these subsections:

- [Section 5.2.1, "Databases Required"](#)

- [Section 5.2.2, "Database Host Requirements"](#)
- [Section 5.2.3, "Database Versions Supported"](#)
- [Section 5.2.4, "Patching the Oracle Database"](#)
- [Section 5.2.5, "About Initialization Parameters"](#)

5.2.1 Databases Required

For Oracle Identity management, a number of separate databases are recommended. [Table 5–1](#) provides a summary of these databases. Which database or databases you use depends on the topology that you are implementing.

The Oracle Metadata Services (MDS) Repository is a particular type of repository that contains metadata for some Oracle Fusion Middleware components. It can also include custom Java EE applications developed by your organization.

Table 5–1 Mapping between Topologies, Databases and Schemas

Topology Type	Database Names	Database Hosts	Service Names	Schemas in Database
Oracle Access Manager 11g and Oracle Identity Manager 11g (OAM11g/OIM11g)	OIDDB	OIDDBHOST1 OIDDBHOST2	oidedg.mycom pany.com	ODS
	IDMDB	IDMDBHOST1 IDMDBHOST2	oamedg.mycom pany.com oimedg.mycom pany.com	OAM, IAU, ORASDPM, MDS ¹ , OIM, SOAINFRA
	IDMDB	IDMDBHOST1 IDMDBHOST2	oamedg.mycom pany.com oimedg.mycom pany.com	OAM, IAU, ORASDPM, MDS, OIM, SOAINFRA
Oracle Identity Federation 11g (OIF11g/OAM11g)	OIDDB	OIDDBHOST1 OIDDBHOST2	oidedg.mycomp any.com	ODS
	IDMDB	IDMDBHOST1 IDMDBHOST2	oifedg.mycom pany.com	OIF

¹ The SOA and Oracle Identity Manager components share the MDS repository.

Notes: If you are using Oracle Internet Directory to store both your identity and policy information, and separating this information across two Oracle Internet Directory instances, then two databases are required for the ODS schema.

The following sections apply to all the databases listed in [Table 5–1](#).

5.2.2 Database Host Requirements

The database used to store the metadata repository should be highly available in its own right, for maximum availability Oracle recommends the use of an Oracle Real Application Clusters (RAC) database.

Ideally the database should use Oracle Automatic Storage Management (ASM) for the storage of data, however this is not necessary.

If using ASM, then ASM should be installed into its own Oracle home and have two disk groups:

- One for the Database Files
- One for the Flash Recovery Area

If you are using Oracle ASM, best practice is to also use Oracle Managed Files.

5.2.3 Database Versions Supported

To check if your database is certified or to see all certified databases, refer to the "Certified Databases" section in the Certification Document:

<http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html>

To determine the version of your installed Oracle Database, execute the following query at the SQL prompt:

```
select version from sys.product_component_version where product like 'Oracle%';
```

5.2.4 Patching the Oracle Database

Patches are required for some versions of Oracle Database.

5.2.4.1 Patch Requirements for Oracle Database 11g (11.1.0.7)

Table 5–2 lists patches required for Oracle Identity Manager configurations that use Oracle Database 11g (11.1.0.7). Before you configure Oracle Identity Manager 11g, be sure to apply the patches to your Oracle Database 11g (11.1.0.7) database.

Table 5–2 Required Patches for Oracle Database 11g (11.1.0.7)

Platform	Patch Number and Description on My Oracle Support
Linux	7614692: BULK FEATURE WITH 'SAVE EXCEPTIONS' DOES NOT WORK IN ORACLE 11G
	7000281: DIFFERENCE IN FORALL STATEMENT BEHAVIOR IN 11G
	8327137: WRONG RESULTS WITH INLINE VIEW AND AGGREGATION FUNCTION
	8617824: MERGE LABEL REQUEST ON TOP OF 11.1.0.7 FOR BUGS 7628358 7598314

5.2.4.2 Patch Requirements for Oracle Database 11g (11.2.0.2.0)

If you are using Oracle Database 11g (11.2.0.2.0), make sure that you download and install the appropriate version (based on the platform) for the RDBMS Patch Number 10259620. This is a prerequisite for installing the Oracle Identity Manager schemas.

Table 5–3 lists the patches required for Oracle Identity Manager configurations that use Oracle Database 11g Release 2 (11.2.0.2.0). Make sure that you download and install the following patches before creating Oracle Identity Manager schemas.

Table 5–3 Required Patches for Oracle Database 11g (11.2.0.2.0)

Platform	Patch Number and Description on My Oracle Support
Linux x86 (32-bit)	RDBMS Interim Patch#10259620.
Linux x86 (64-bit)	

If this patch is not applied, then problems might occur in user and role search and manager lookup. In addition, search results might return empty result.

Note:

- Apply this patch in ONLINE mode. Refer to the readme.txt file bundled with the patch for the steps to be followed.
- In some environments, the RDBMS Interim Patch has been unable to resolve the issue, but the published workaround works. Refer to the metalink note "Wrong Results on 11.2.0.2 with Function-Based Index and OR Expansion due to fix for Bug:8352378 [Metalink Note ID 1264550.1]" for the workaround. This note can be followed to set the parameters accordingly with the only exception that they need to be altered at the Database Instance level by using ALTER SYSTEM SET <param>=<value> scope=<memory> or <both>.

5.2.5 About Initialization Parameters

The databases must have the following minimum initialization parameters defined:

Table 5–4 Minimum Initialization Parameters for Oracle RAC Databases

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	800 ¹
session_max_open_files	50
sessions	500
processes	500
sga_target	512M
pga_aggregate_target	100M
sga_max_size	4G
session_cached_cursors	500

¹ OAM requires a minimum of 800 open cursors in the database. When OIM and OAM are available, the number of open cursors should be 1500.

If the database is being used for Oracle Internet Directory, it must have the following minimum initialization parameters defined:

Table 5–5 Minimum Initialization Parameters for Oracle RAC Oracle Internet Directory Databases

Parameter	Value
aq_tm_processes	1
dml_locks	200
job_queue_processes	10
open_cursors	800
session_max_open_files	50
sessions	500
processes	2500
sga_target	4G
pga_aggregate_target	2G
sga_max_size	4G
session_cached_cursors	500
_b_tree_bitmap_plans	FALSE

Note: For guidelines on setting up optimum parameters for the Database, see *Oracle Fusion Applications Performance and Tuning Guide*.

5.3 Installing the Database for an Enterprise Deployment

Install and configure the database repository as follows.

Oracle Clusterware

- For 10g Release 2 (10.2), see the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in ["Related Documents"](#).
- For 11g Release 1 (11.1), see *Oracle Clusterware Installation Guide*.

Automatic Storage Management

- For 10g Release 2 (10.2), see the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in ["Related Documents"](#).
- For 11g Release 1 (11.1), see *Oracle Clusterware Installation Guide*.
- When you run the installer, select the **Configure Automatic Storage Management** option in the **Select Configuration** screen to create a separate Automatic Storage Management home.

Oracle Real Application Clusters

- For 10g Release 2 (10.2), see the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Installation Guide* for your platform, listed in ["Related Documents"](#).
- For 11g Release 1 (11.1), see *Oracle Real Application Clusters Installation Guide*.

Oracle Real Application Clusters Database

Create a Real Applications Clusters Database with the following characteristics:

- Database must be in archive log mode to facilitate backup and recovery.
- Optionally, enable the Flashback database.
- Create UNDO tablespace of sufficient size to handle any rollback requirements during the Oracle Identity Manager reconciliation process.
- Database is created with ALT32UTF8 character set.

5.4 Creating Database Services

This section describes how to configure the database for Oracle Fusion Middleware 11g metadata. It contains the following topics:

- [Section 5.4.1, "Creating Database Services for 10.x and 11.1.x Databases"](#)
- [Section 5.4.2, "Creating Database Services for 11.2.x Databases"](#)
- [Section 5.4.3, "Database Tuning"](#)

5.4.1 Creating Database Services for 10.x and 11.1.x Databases

For complete instructions on creating database services, see the chapter on Workload Management in the *Oracle Database Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide*. Oracle recommends that a specific database service be used for a product suite, even when product suites share the same database. It is also recommended that the database service used is different than the default database service.

Use the `CREATE_SERVICE` subprogram to create the database services for the components in your topology. The lists of services to be created are listed in [Section 5-1, "Mapping between Topologies, Databases and Schemas."](#)

1. Log on to SQL*Plus as the `sysdba` user by typing:

```
sqlplus "sys/password as sysdba"
```

Then run the following command to create a service called `oamedg.mycompany.com` for Oracle Access Manager:

```
EXECUTE DBMS_SERVICE.CREATE_SERVICE  
(SERVICE_NAME => 'oamedg.mycompany.com',  
NETWORK_NAME => 'oamedg.mycompany.com');
```

2. Add the service to the database and assign it to the instances using `srvctl`:

```
srvctl add service -d idmdb -s oamedg.mycompany.com -r idmdb1,idmdb2
```

3. Start the service using `srvctl`:

```
srvctl start service -d idmdb -s oamedg.mycompany.com
```

When creating a service in the database for Oracle Internet Directory, ensure that the service is enabled for high-availability notifications and configured with the proper server-side Transparent Application Failover (TAF) settings. Use the `DBMS_SERVICE` package to create the service to enable high availability notification to be sent through Advanced Queuing (AQ) by setting the `AQ_HA_NOTIFICATIONS` attribute to `TRUE` and configure server-side Transparent Application Failover (TAF) settings, as follows:

1. Use the `CREATE_SERVICE` subprogram to both create the database service and enable high-availability notification and configure server-side Transparent Application Failover (TAF) settings.

Log on to SQL*Plus as the `sysdba` user by typing:

```
sqlplus "sys/password as sysdba"
```

Then execute this command:

```
EXECUTE
DBMS_SERVICE.CREATE_SERVICE(
SERVICE_NAME => 'oidedg.mycompany.com',
NETWORK_NAME => 'oidedg.mycompany.com',
AQ_HA_NOTIFICATIONS => TRUE,
FAILOVER_METHOD => DBMS_SERVICE.FAILOVER_METHOD_BASIC,
FAILOVER_TYPE => DBMS_SERVICE.FAILOVER_TYPE_SELECT,
FAILOVER_RETRIES => 5, FAILOVER_DELAY => 5);
```

Note: The `EXECUTE DBMS_SERVICE` command shown must be entered on a single line to execute properly.

For more information about the `DBMS_SERVICE` package, see the *Oracle Database PL/SQL Packages and Types Reference*.

2. Add the service to the database and assign it to the instances using `srvctl`:

```
srvctl add service -d oiddb -s oidedg.mycompany.com -r oiddb1,oiddb2
```

3. Start the service using `srvctl`:

```
srvctl start service -d oiddb -s oidedg.mycompany.com
```

Note: For more information about the `SRVCTL` command, see the *Oracle Real Application Clusters Administration and Deployment Guide*.

5.4.2 Creating Database Services for 11.2.x Databases

Use `srvctl` to create the database services for the components in your topology. The lists of services to be created are listed in [Table 5-1, "Mapping between Topologies, Databases and Schemas"](#).

1. Create service using the command `srvctl add service`, as follows.

```
srvctl add service -d oiddb -s oidedg.mycompany.com -r idmdb1,idmdb2 -q TRUE -m
BASIC -e SELECT -w 5 -z 5
```

The meanings of the command-line arguments are as follows:

Option	Argument
-d	Unique name for the database
-s	Service name
-r	Comma separated list of preferred instances
-q	AQ HA notifications (TRUE or FALSE)

Option	Argument
-e	Failover type (NONE, SESSION, or SELECT)
-m	Failover method (NONE or BASIC)
-w	Failover delay (integer)
-z	Failover retries (integer)

Note: Transparent Application Failover (TAF) settings are only required when creating a service for Oracle Internet Directory.

2. Start the Service using `srvctl start service`

```
srvctl start service -d oiddb -s oidedg.mycompany.com
```

3. Validate the service started by using `srvctl status service`, as follows:

```
srvctl status service -d oiddb -s oidedg.mycompany.com
Service oidedg.mycompany.com is running on instance(s) idmdb1,idmdb2
```

4. Validate that the service was created correctly by using `srvctl config service`:

```
srvctl config service -d oiddb -s oidedg.mycompany.com
Service name: oidedg.mycompany.com
Service is enabled
Server pool: oiddb_oidedg.mycompany.com
Cardinality: 2
Disconnect: false
Service role: PRIMARY
Management policy: AUTOMATIC
DTP transaction: false
AQ HA notifications: true
Failover type: SELECT
Failover method: BASIC
TAF failover retries: 5
TAF failover delay: 5
Connection Load Balancing Goal: LONG
Runtime Load Balancing Goal: NONE
TAF policy specification: NONE
Edition:
Preferred instances: idmdb1,idmdb2
Available instances:
```

Note: For more information about the SRVCTL command, see the *Oracle Real Application Clusters Administration and Deployment Guide*.

5.4.3 Database Tuning

The database parameters defined in [Section 5.3, "Installing the Database for an Enterprise Deployment"](#) are only a guide. You might need to perform additional tuning after the system is in use. For more information, see *Database Performance Tuning Guide*.

Refresh the database statistics after you initially load the database, and on an ongoing basis. To do that, issue the following SQL*Plus command:

```
exec DBMS_STATS.GATHER_SCHEMA_STATS (OWNNAME=> '<OIM_SCHEMA>', ESTIMATE_
PERCENT=>DBMS_STATS.AUTO_SAMPLE_SIZE, DEGREE=>8, OPTIONS=>'GATHER AUTO', NO_
INVALIDATE=>FALSE);
```

5.5 Loading the Identity Management Schemas in the Oracle RAC Database by Using RCU

You run RCU to create the collection of schemas used by Identity Management and Management Services.

1. Start RCU by issuing this command:

```
RCU_HOME/bin/rcu &
```

2. On the Welcome screen, click **Next**.
3. On the Create Repository screen, select the **Create** operation to load component schemas into a database. Then click **Next**.
4. On the Database Connection Details screen, provide the information required to connect to an existing database. For example:

Database Type: Oracle Database

- **Host Name:** Enter one of the Oracle RAC nodes. Specify the Virtual IP name. For example: OIDDBHOST1-vip.mycompany.com.
- **Port:** The port number for the database listener. For example: 1521
- **Service Name:** The service name of the database. For example oidedg.mycompany.com.
- **Username:** sys
- **Password:** The sys user password
- **Role:** SYSDBA

Click **Next**.

5. On the Check Prerequisites screen, click **OK** after the prerequisites have been validated.
6. On the Select Components screen, provide the following values:
Create a New Prefix: Enter a prefix to be added to the database schemas. Note that all schemas except for the ODS schema are required to have a prefix. For example, enter EDG.
Components: Select the schemas shown in [Table 5–6](#).

Table 5–6 Component Schemas

Product	RCU Option	Service Name	Comments
Oracle Internet Directory	Identity Management–Oracle Internet Directory	oidedg.mycompany.com	

Table 5–6 (Cont.) Component Schemas

Product	RCU Option	Service Name	Comments
Oracle Access Manager	Identity Management–Oracle Access Manager	oamedg.mycompany.com	Audit Services will also be selected.
Oracle Identity Manager	Identity Management–Oracle Identity Manager	oamedg.mycompany.com	Metadata Services, SOA infrastructure, and User Messaging will also be selected.
Oracle Identity Federation	Identity Management–Oracle Identity Federation	oifedg.mycompany.com	

Click **Next**.

Notes: If your topology requires more than one database, the following important considerations apply:

- Be sure to install the correct schemas in the correct database.
 - You might have to run the RCU more than once to create all the schemas for a given topology.
 - [Table 5–1](#) in this chapter provides the recommended mapping between the schemas and their corresponding databases. Refer to this table to ensure that the correct details are entered in this screen.
-

7. On the Check Prerequisites screen, click **OK** after the prerequisites have been validated.
8. On the Schema Passwords screen, enter the passwords for the schemas. You can choose to use either the same password for all the schemas or different passwords for each of the schemas. Oracle recommends choosing different passwords for different schema's to enhance security

Click **Next**.

9. On the Map Tablespaces screen, accept the defaults and click **Next**.
10. On the confirmation screen, click **OK** to allow the creation of the tablespaces.
11. On the Creating tablespaces screen, click **OK** to acknowledge creation of the tablespaces.
12. On the Summary screen, the summary and verify that the details provided are accurate. Click **Create** to start the schema creation process.
13. On the Completion summary screen, verify that the schemas were created.

Click **Close** to exit.

5.6 Backing up the Database

After you have prepared your database, back it up. You can back up your database using the appropriate RMAN commands for your environment. See *Oracle Database Backup and Recovery User's Guide*.

Installing the Software for an Enterprise Deployment

This chapter describes the software installations required for an Oracle Identity Management enterprise deployment.

This chapter contains the following topics:

- [Section 6.1, "Overview of the Software Installation Process"](#)
- [Section 6.2, "Installing Oracle HTTP Server"](#)
- [Section 6.3, "Installing Oracle Fusion Middleware"](#)

6.1 Overview of the Software Installation Process

The installation is divided in two sections. In the first one, the WebTier required installations are addressed. In the second, the required Oracle Fusion Middleware components are installed. Later chapters describe the configuration steps to create the Oracle Identity Management topology.

See Also: *The Oracle Fusion Middleware 11g Release 1 Download, Installation, and Configuration Readme* for this release, at:
http://docs.oracle.com/cd/E23104_01/download_readme.htm

6.1.1 Obtaining the Software

Oracle groups its software releases by product area. A **Product Media Pack** refers to those groupings. Each media pack may also include a zipped file containing electronic documentation files or "Quick Install" files, which facilitate the initial installation of the software.

Note: For installations of Oracle Fusion Applications, you must have available the complete set of software contained in the product media pack. You cannot install from individual pieces. Therefore, if you need to install from media that is no longer available on Oracle Software Delivery Cloud, contact My Oracle Support to obtain the complete media pack.

Once you have completed the software licensing agreements, you can obtain the Oracle Fusion Applications software using one of these two methods:

- **Oracle Software Delivery Cloud Portal:** Provides you with a readme document that helps you to determine which media you need to fulfill the license you have purchased. You download only the media you need. This is the default delivery method.
- **Oracle Store:** Provides a complete set of the software in DVD format. You use only the DVDs covered by your software licensing agreement.

Using either method, you can obtain the Oracle Fusion Applications Provisioning repository and gain access to the Oracle Fusion Applications documentation library.

After you download the archive file, extract the archive file into a directory of your choice on the machine where you are performing the installation.

For more information, see the Preparing for an Installation chapter in *Oracle Fusion Applications Installation Guide*.

6.1.2 Software to Install

Different topologies use different servers and require different software to be installed. [Table 6–1, "Software to be Installed for Different Topologies"](#) shows, for each topology, which software should be installed into each host. The subsequent sections explain how to do this. Also see [Table 2–2, "Software Versions Used"](#) a

Where two different pieces of Oracle binary software are installed onto the same host (for example OIM11g and SOA11g), this software is installed in the same Middleware home location, but in different Oracle homes.

All software uses the same Middleware home location.

Notes:

- When using shared storage, ensure that users and groups used in the installation have the same ID on all hosts that use the storage. If you fail to do this, some hosts might not be able to see or execute some all the files.
 - Some products, such as Oracle Internet Directory and Oracle Virtual Directory, require you to run a script that sets the permissions of some files to `root`.
-
-

Table 6–1 Software to be Installed for Different Topologies

Topology	Hosts	OHS 11g	JRockit	WLS	IAM	SOA	IDM
All	WEBHOST1	X					
	WEBHOST2	X					
OAM11g/OIM11g	IDMHOST1		X	X	X	X	X
	IDMHOST2		X	X	X	X	X
	OIMHOST1		X	X	X	X	
	OIMHOST2		X	X	X	X	
	LDAPHOST1		X	X			X

Table 6–1 (Cont.) Software to be Installed for Different Topologies

Topology	Hosts	OHS 11g	JRockit	WLS	IAM	SOA	IDM
	LDAPHOST2		X	X			X
Split Domain for OIM (Separate MW_ HOME, SOA, and IAM) (Separate MW_ HOME, SOA, and IAM)	IDMHOST1		X	X	X		X
	IDMHOST2		X	X	X		X
	OIMHOST1		X	X	X	X	
	OIMHOST2		X	X	X	X	
	LDAPHOST1		X	X			X
	LDAPHOST2		X	X			X
	IDMHOST2		X	X	X	X	X
	OIMHOST1		X	X	X	X	
OIF11g/OAM11g	OIMHOST2		X	X	X	X	
	LDAPHOST1		X	X			X
	LDAPHOST2		X	X			X

Oracle Identity Management products are bundled as two product sets: Oracle Identity Management and Oracle Identity and Access Management. (See [Table 2–2, "Software Versions Used"](#).) The relevant Identity Management software is installed into separate Oracle homes.

6.2 Installing Oracle HTTP Server

This section explains how to install Oracle HTTP Server on WEBHOST1 and WEBHOST2.

This section contains the following topics:

- [Section 6.2.1, "Verifying Prerequisites"](#)
- [Section 6.2.2, "Running the Installer"](#)
- [Section 6.2.3, "Backing Up the Installation"](#)

6.2.1 Verifying Prerequisites

Prior to installing the Oracle HTTP server, check that your machines meet the following requirements:

1. Ensure that the system, patch, kernel, and other requirements are met as specified in *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

2. On Linux platforms, if the `/etc/oraInst.loc` file exists, check that its contents are correct, as described in [Section 6.2.1.1, "Check oraInst.loc."](#)

6.2.1.1 Check oraInst.loc

Check that the inventory directory is correct and that you have write permissions for that directory. If the `/etc/oraInst.loc` file does not exist, you can skip this step.

The contents of the `oraInst.loc` file are shown in this example:

```
inventory_loc=/u01/app/oraInventory
inst_group=oinstall
```

6.2.2 Running the Installer

As described in [Section 4.4.4, "Directory Structure,"](#) you install the Oracle HTTP Server onto a local disk. You can install it on shared storage, but if you do that, you must allow access from the Web Tier DMZ to your shared disk array, which is undesirable. If you decide to install onto shared disk then please see the Release Notes for further configuration information.

Before Starting the install, ensure that the following environment variables are not set on Linux platforms.

- `LD_ASSUME_KERNEL`
- `ORACLE_INSTANCE`

To start Oracle Universal Installer on Linux, change directory to Disk 1 of the installation media and issue the command

```
./runInstaller
```

To start Oracle Universal Installer on Windows, navigate to Disk 1 of the installation media in Windows Explorer and double-click `setup.exe`.

On the Specify Inventory Directory screen, do the following:

- Enter `HOME/oraInventory`, where *HOME* is the home directory of the user performing the installation (this is the recommended location).
- Enter the OS group for the user performing the installation.
- Click **Next**.

Follow the instructions on screen to execute `createCentralInventory.sh` as root.

Click **OK**.

Proceed as follows:

1. On the Specify Oracle Inventory Directory screen, enter `HOME/oraInventory`, where *HOME* is the home directory of the user performing the installation. (This is the recommended location).

Enter the OS group for the user performing the installation.

Click **Next**.
2. On the Welcome screen, click **Next**.
3. On the Select Installation Type screen, select **Install Software -> Do Not Configure**

Click **Next**.

4. On the Prerequisite Checks screen, click **Next**.
5. On the Specify Installation Location screen, specify the following values:
 - **Fusion Middleware Home Location (Installation Location)** For example:
`/u01/app/oracle/product/fmw`
 - **Oracle Home Location Directory:** `web`
6. On the Specify Security Updates screen, choose whether to receive security updates from Oracle support.
 Click **Next**.
7. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Install**.

6.2.3 Backing Up the Installation

The Fusion Middleware Home should be backed up now (make sure no server is running at this point):

```
tar -cvpf fmwhomeback.tar ORACLE_BASE/product/fmw HOME/oraInventory
```

6.3 Installing Oracle Fusion Middleware

This section describes how to install Oracle Fusion Middleware.

This section contains the following topics:

- [Section 6.3.1, "Installing Oracle Fusion Middleware Components"](#)
- [Section 6.3.2, "Installing Oracle Fusion Middleware Home"](#)
- [Section 6.3.3, "Installing Oracle WebLogic Server and Creating the Fusion Middleware Home"](#)
- [Section 6.3.4, "Installing Oracle Identity Management"](#)
- [Section 6.3.5, "Installing the Oracle SOA Suite"](#)
- [Section 6.3.6, "Installing Oracle Identity and Access Management"](#)
- [Section 6.3.7, "Applying Patches and Workarounds"](#)
- [Section 6.3.8, "Backing Up the Installation"](#)

Note: Oracle Identity Management products are bundled as two product sets: Oracle Identity Management and Oracle Identity and Access Management.

6.3.1 Installing Oracle Fusion Middleware Components

This section describes how to install the required binaries to create the Middleware home (*MW_HOME*), the Oracle WebLogic Server home (*WL_HOME*), the Oracle homes for Oracle Identity Management (*IDM_ORACLE_HOME*), the Oracle SOA Suite (*SOA_ORACLE_HOME*) and Oracle Identity and Access Management (*IAM_ORACLE_HOME*). A summary of these homes is provided in [Table 6–2, "Summary of Homes"](#).

Table 6–2 Summary of Homes

Home Name	Home Description	Products Installed
<i>MW_HOME</i> ¹	Consists of the Oracle WebLogic Server home and, optionally, one or more Oracle homes.	
<i>WL_HOME</i>	This is the root directory in which Oracle WebLogic Server is installed. The <i>WL_HOME</i> directory is a peer of Oracle home directory and resides within the <i>MW_HOME</i> .	Oracle WebLogic Server
<i>IDM_ORACLE_HOME</i>	Contains the binary and library files for Oracle Identity Management and is located in: <i>MW_HOME/idm</i>	Oracle Internet Directory Oracle Virtual Directory Oracle Directory Services Manager Oracle Identity Federation
<i>IAM_ORACLE_HOME</i>	Contains the binary and library files required for Oracle Identity and Access Management and is located in <i>MW_HOME/iam</i> .	Oracle Access Manager Oracle Identity Management
<i>SOA_ORACLE_HOME</i>	Contains the binary and library files required for the Oracle SOA Suite. Required only when creating topologies with OIM and is located in <i>MW_HOME/soa</i> .	Oracle SOA Suite
<i>ORACLE_COMMON_HOME</i>	Contains the generic Oracle home files. This Oracle home is created automatically by any product installation and is located in <i>MW_HOME/oracle_common</i> .	Generic commands

¹ Different topologies require multiple *MW_HOME*s with different software installed. The *MW_HOME*, however, is always mounted at the same location, for example: */u01/app/oracle/product/fmw*

If you are deploying Oracle Identity Manager in a split domain, install the IAM and SOA binaries twice, once for each domain, using a separate *MW_HOME* in the Oracle Identity Manager domain for one set.

Oracle strongly recommends that you read the release notes for any additional installation and deployment considerations prior to starting the setup process.

6.3.2 Installing Oracle Fusion Middleware Home

As described in [Section 4.4.4, "Directory Structure,"](#) you install Oracle Fusion Middleware software in at least two storage locations for redundancy.

You must install the following components of Oracle Fusion Middleware to create a Middleware home (*MW_HOME*):

1. Oracle WebLogic Server: [Section 6.3.3, "Installing Oracle WebLogic Server and Creating the Fusion Middleware Home"](#)
2. One or more of the Oracle Fusion Middleware components
 - a. [Section 6.3.4, "Installing Oracle Identity Management"](#)
 - b. [Section 6.3.6, "Installing Oracle Identity and Access Management"](#)
 - c. [Section 6.3.5, "Installing the Oracle SOA Suite"](#)
3. Oracle Fusion Middleware for Identity Management

6.3.3 Installing Oracle WebLogic Server and Creating the Fusion Middleware Home

Perform these steps to install the Oracle WebLogic Server.

To install Oracle WebLogic Server, proceed as follows:

Note: If you are installing WebLogic Server on a 64-bit platform using a 64-bit JDK, follow the steps in section "Installing WebLogic Server on 64-Bit Platforms Using a 64-Bit JDK" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* instead of the steps in this section.

1. Start the installer for Oracle WebLogic Server from the installation media:

```
./wls1036_linux32.bin
```

2. In the Welcome screen, click **Next**.

3. In the Choose Middleware Home Directory screen, do the following:

- Select **Create a new Middleware Home**.
- For Middleware Home Directory, enter **ORACLE_BASE/product/fmw**

ORACLE_BASE is the base directory under which Oracle products are installed. The recommended value is `/u01/app/oracle`. See [Section 4.4, "About Recommended Locations for the Different Directories"](#) for more information.

Click **Next**.

4. In the Register for Security Updates screen, enter your contact information so that you can be notified of security updates, and click **Next**.
5. In the Choose Install Type screen, select **Custom**, and click **Next**.
6. In the Choose Products and Components screen, click **Next**.
7. In the JDK Selection screen, select *only* **Oracle JRockit 1.6.0_version SDK**, and click **Next**.
8. In the Choose Product Installation Directories screen, accept the directories **ORACLE_BASE/product/fmw/wlserver_10.3** and **ORACLE_BASE/product/fmw/coherence_3.7**, and click **Next**.
9. In the Installation Summary screen, click **Next**.

The Oracle WebLogic Server software is installed.

10. In the Installation Complete screen, clear the **Run Quickstart** check box and click **Done**.

11. Validate the installation by verifying that the following directories and files appear in the ORACLE_HOME directory after installing Oracle WebLogic Server:

- coherence_version
- jrockit-jdkversion
- modules
- registry.xml
- utils
- domain-registry.xml

- logs
- ocm.rsp
- registry.dat
- wlsserver_10.3

6.3.4 Installing Oracle Identity Management

Perform these steps to install Oracle Identity Management on the hosts identified in [Table 6–1, "Software to be Installed for Different Topologies"](#).

Oracle Identity Management consists of:

- Oracle Internet Directory
- Oracle Virtual Directory
- Oracle Directory Services Manager (ODSM)
- Oracle Identity Federation

Note: Because the installation is performed on shared storage, the two *MW_HOME* installations are accessible and used by the remaining servers in that tier of the topology.

When provisioning the software on the local hard disk of the machine, ensure you complete the steps on all the hosts in the tier.

Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

To start the Oracle Fusion Middleware 11g Oracle Identity Management Installer, change directory to Disk 1 of the installation media and enter the command:

```
./runInstaller
```

Then proceed as follows:

1. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:

- **Specify the Inventory Directory:** /u01/app/oraInventory
- **Operating System Group Name:** oinstall

A dialog box appears with the following message:

```
Certain actions need to be performed with root privileges before the
install can continue. Please execute the script
/u01/app/oraInventory/createCentralInventory.sh now from another window and
then press "Ok" to continue the install. If you do not have the root
privileges and wish to continue the install select the "Continue
installation with local inventory" option.
```

Log in as root and run:

```
/u01/app/oraInventory/createCentralInventory.sh
```


This sets the required permissions for the Oracle Inventory Directory and then brings up the Welcome screen.

Note: The Oracle Inventory screen is not shown if an Oracle product was previously installed on the host. If the Oracle Inventory screen is not displayed for this installation, ensure that the following are true:

1. The `/etc/oraInst.loc` file exists.
 2. The Inventory directory listed is valid.
 3. The user performing the installation has write permissions for the Inventory directory.
-

2. On the Welcome screen, click **Next**.
3. On the **Install Software Updates** screen, choose whether to register with Oracle Support for updates or search for updates locally.
Click **Next**.
4. On the Select Installation Type screen, select **Install Software - Do Not Configure**, and then click **Next**.
5. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.
6. On the Specify Installation Location screen, enter the following values:
 - **Oracle Middleware Home:** Select the previously installed Middleware home from the list for `MW_HOME`, for example:
`/u01/app/oracle/product/fmw`
 - **Oracle Home Directory:** Enter `idm` as the Oracle home directory name.
 Click **Next**.
7. On the Installation Summary screen, click **Install - Do Not Configure**.
8. On the Installation Progress screen, on Linux systems, a dialog box appears that prompts you to run the `oracleRoot.sh` script. Open a window and run the `oracleRoot.sh` script, as the `root` user.
9. On the Installation Complete screen, click **Finish**.

6.3.5 Installing the Oracle SOA Suite

Perform these steps to install the Oracle SOA Suite.

Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle SOA Suite* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

To start the Oracle Fusion Middleware 11g SOA Suite Installer, change directory to Disk 1 of the installation media and enter the appropriate command.

On Linux systems the command is:

```
./runInstaller
```

On Windows, the command is:

```
setup.exe
```

When the installer prompts you for a JRE/JDK location, enter the Oracle SDK location created in the Oracle WebLogic Server installation, for example:

```
/u01/app/oracle/product/fmw/jrockit_version
```

Then perform these installation steps:

1. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:
 - **Specify the Inventory Directory:** /u01/app/oraInventory
 - **Operating System Group Name:** oinstall

A dialog box appears with the following message:

```
Certain actions need to be performed with root privileges before the install
can continue. Please execute the script
/u01/app/oraInventory/createCentralInventory.sh now from another window and
then press "Ok" to continue the install. If you do not have the root privileges
and wish to continue the install select the "Continue installation with local
inventory" option.
```

Log in as root and run:

```
/u01/app/oraInventory/createCentralInventory.sh
```

This sets the required permissions for the Oracle Inventory Directory and then brings up the Welcome screen.

Note: The Oracle Inventory screen is not shown if an Oracle product was previously installed on the host. If the Oracle Inventory screen is not displayed for this installation, check the following:

1. The /etc/oraInst.loc file exists.
 2. The Inventory directory listed is valid.
 3. The user performing the installation has write permissions for the Inventory directory.
-
-

2. On the Welcome screen, click **Next**.
3. On the **Install Software Updates** screen, choose whether to register with Oracle Support for updates or search for updates locally.

Click **Next**.

4. On the Prerequisite Checks screen, verify that the checks complete successfully, and then click **Next**.
5. On the Specify Installation Location screen, enter the following values:
 - **Oracle Middleware Home:** Select a previously installed Middleware Home from the drop-down list. For example: /u01/app/oracle/product/fmw
 - **Oracle Home Directory:** Enter SOA as the Oracle home directory name.

Note: You must use the same Oracle home directory name for Oracle SOA Suite on all hosts.

6. Click **Next**.

7. On the Application Server screen, choose your Application Server, for example: Web Logic Server.
Click **Next**.
8. On the Installation Summary screen, click **Install**.
9. On the Installation Process screen, click **Next**.
10. On the Installation Complete screen, click **Finish**.

6.3.6 Installing Oracle Identity and Access Management

Oracle Identity and Access Management consists of the following products:

- Oracle Access Manager 11g
- Oracle Identity Manager

Perform the steps in this section to install Oracle Identity and Access Management on the hosts identified in [Table 2-2, "Software Versions Used"](#).

Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.

To start the Oracle Fusion Middleware 11g Installer for Oracle Identity and Access Management, change directory to Disk 1 of the installation media and enter the command:

```
./runInstaller
```

When the installer prompts you for a JRE/JDK location, enter the Oracle SDK location created in the Oracle WebLogic Server installation, for example:

```
/u01/app/oracle/product/fmw/jrockit_version
```

Then perform these installation steps:

1. On the Specify Inventory Directory screen, enter values for the Oracle Inventory Directory and the Operating System Group Name. For example:
 - **Specify the Inventory Directory:** /u01/app/oraInventory
 - **Operating System Group Name:** oinstall

A dialog box appears with the following message:

```
Certain actions need to be performed with root privileges before the install
can continue. Please execute the script
/u01/app/oraInventory/createCentralInventory.sh now from another window and
then press "Ok" to continue the install. If you do not have the root privileges
and wish to continue the install select the "Continue installation with local
inventory" option.
```

Log in as root and run:

```
/u01/app/oraInventory/createCentralInventory.sh
```

This sets the required permissions for the Oracle Inventory Directory and then brings up the Welcome screen.

Note: The Oracle Inventory screen is not shown if an Oracle product was previously installed on the host. If the Oracle Inventory screen is not displayed for this installation, check the following:

1. The `/etc/oraInst.loc` file exists.
 2. The Inventory directory listed is valid.
 3. The user performing the installation has write permissions for the Inventory directory.
-

2. On the Welcome screen click **Next**.
3. On the Install Software Updates screen, choose whether to register with Oracle Support for updates or to search for updates locally.
4. On the Prerequisite Checks screen, verify that the checks complete successfully, then click **Next**.
5. On the Specify Installation Location screen, enter the following values:
 - **Oracle Middle Ware Home:** Select a previously installed Middleware Home from the drop-down list. For example: `/u01/app/oracle/product/fmw`
 - **Oracle Home Directory:** Enter `iam` as the Oracle home directory name.Click **Next**.
6. On the Installation Summary screen, click **Install**.
7. On the Installation Progress screen, click **Next**.
8. On the Installation Complete screen, click **Finish**.

6.3.7 Applying Patches and Workarounds

You must apply the following patches and workarounds to your environment. Patches are available for download from <http://support.oracle.com>. You can find instructions for deploying each patch in the enclosed `README.html` file.

For a complete list of patches, see the Oracle Fusion Middleware Release Notes for your platform and operating system.

This section contains the following topics:

- [Section 6.3.7.1, "Patches for Fusion Middleware"](#)
- [Section 6.3.7.2, "Provisioning the OIM Login Modules Under the WebLogic Server Library Directory"](#)
- [Section 6.3.7.3, "Creating the wfullclient.jar File"](#)

6.3.7.1 Patches for Fusion Middleware

The Release Notes for this version of Oracle Fusion Applications contain the list of Oracle Fusion Middleware patches to apply. You must apply the patches to ensure that your software operates as expected.

6.3.7.2 Provisioning the OIM Login Modules Under the WebLogic Server Library Directory

Due to issues with versions of the configuration wizard, some environmental variables are not added to the `ASERVER_HOME/bin/setDomainenv.sh` script. This causes certain install sequences to fail. This section is a temporary workaround for that

problem. The steps in this section must be performed on all the hosts in application tier (IDMHOST1, IDMHOST2, OIMHOST1, and OIMHOST2).

Apply the following steps across all the WebLogic Server homes in the domain.

1. Copy the `OIMAuthenticator.jar`, `oimmbean.jar`, `oimsgmbean.jar` and `oimsignaturemban.jar` files located under the `IAM_ORACLE_HOME/server/loginmodule/wls` directory to the `MW_HOME/wlserver_10.3/server/lib/mbeantypes` directory.

```
cp $IAM_ORACLE_HOME/server/loginmodule/wls/* $MW_HOME/wlserver_10.3/server/lib/mbeantypes/.
```

2. Change directory to `MW_HOME/wlserver_10.3/server/lib/mbeantypes/`.

```
cd $MW_HOME/wlserver_10.3/server/lib/mbeantypes
```

3. Change the permissions on these files to 750 by using the `chmod` command.

```
chmod 750 *
```

6.3.7.3 Creating the `wlfullclient.jar` File

Oracle Identity Manager uses the `wlfullclient.jar` library for certain operations. Oracle does not ship this library, so you must create this library manually. Oracle recommends creating this library under the `MW_HOME/wlserver_10.3/server/lib` directory on all the machines in the application tier of your environment. You do not need to create this library on directory tier machines such as `LDAPHOST1` and `LDAPHOST2`.

Follow these steps to create the `wlfullclient.jar` file:

1. Navigate to the `MW_HOME/wlserver_10.3/server/lib` directory
2. Set your `JAVA_HOME` environment variable and ensure that the `JAVA_HOME/bin` directory is in your path.
3. Create the `wlfullclient.jar` file by running:

```
java -jar wljarbuilder.jar
```

6.3.8 Backing Up the Installation

It is a best practice recommendation to back up the Middleware Home and the Oracle Homes. On Linux, to create a backup of the `MW_HOME` and the `ORACLE_HOMES`, as the root user, type:

```
tar -cvpf fmwhomeback.tar ORACLE_BASE/product/fmw
```

This creates a backup of the installation files for any products installed in the Oracle Fusion Middleware home.

Configuring the Web Tier for an Enterprise Deployment

This chapter describes how to configure the Oracle Web Tier for an Oracle Identity Management enterprise deployment.

This chapter includes the following topics:

- [Section 7.1, "Overview of Configuring the Web Tier"](#)
- [Section 7.2, "Prerequisites for Configuring the Web Tier"](#)
- [Section 7.3, "Running the Configuration Wizard to Configure the HTTP Server"](#)
- [Section 7.4, "Validating the Configuration"](#)
- [Section 7.5, "Configuring Virtual Hosts and Server Owner"](#)
- [Section 7.6, "Backing up the Web Tier Configuration"](#)

7.1 Overview of Configuring the Web Tier

This chapter describes how to associate the Oracle Web Tier with the WebLogic Server domain. Once the Web tier is associated with the WebLogic Server, you can monitor it using the Oracle Fusion Middleware Console.

You then configure the load balancer to route all HTTP requests to WEBHOST1 and WEBHOST2.

The last section describes how to define the Oracle HTTP Server directives to route requests to the load balancer virtual hosts you defined in [Chapter 3, "Preparing the Network for an Enterprise Deployment."](#)

7.2 Prerequisites for Configuring the Web Tier

- Before configuring the Oracle Web Tier software, you must install it on WEBHOST1 and WEBHOST2, as described in [Section 6.2, "Installing Oracle HTTP Server."](#) Run the Configuration Wizard to define the instance home, the instance name, and the Oracle HTTP Server component name.
- Ensure that port 7777 is not in use. Because Oracle HTTP Server is installed by default on port 7777, you must ensure that port 7777 is not used by any other service on the nodes. To check if this port is in use, run the following command before installing Oracle HTTP Server. You must free the port if it is in use.

```
netstat -an | grep 7777
```

- Create a file containing the ports used by Oracle HTTP Server. On Disk1 of the installation media, locate the file `stage/Response/staticports.ini`. Copy it to a file called `ohs_ports.ini`. Delete all entries in `ohs_ports.ini` except for `OHS_PORT` and `OPMN_Local_Port`. Change the values of those ports to 7777 and 6700, respectively.

Note: If the port names in the file are slightly different from `OHS_PORT` and `OPMN_Local_Port`, use the names in the file.

7.3 Running the Configuration Wizard to Configure the HTTP Server

The steps for configuring the Oracle Web Tier are the same for `WEBHOST1` and `WEBHOST2`.

Perform these steps to configure the Oracle web tier:

1. Change the directory to the location of the Oracle Fusion Middleware Configuration Wizard:

```
cd WEB_ORACLE_HOME/bin
```

2. Start the Configuration Wizard:

```
./config.sh
```

Enter the following information into the configuration wizard:

1. On the Welcome screen, click **Next**.
2. On the Configure Component screen, select: **Oracle HTTP Server**.

Ensure that Associate Selected Components with WebLogic Domain is **NOT** selected.

Ensure Oracle Web Cache is **NOT** selected.

Click **Next**.

3. On the Specify Component Details screen, specify the following values:

Enter the following values for `WEBHOST1`:

- Instance Home Location: `/u01/app/oracle/admin/web1`
- Instance Name: `web1`
- OHS Component Name: `ohs1`

Enter the following values for `WEBHOST2`:

- Instance Home Location: `/u01/app/oracle/admin/web2`
- Instance Name: `web2`
- OHS Component Name: `ohs2`

Click **Next**.

4. On the Configure Ports screen, you use the `ohs_ports.ini` file you created in [Section 7.2, "Prerequisites for Configuring the Web Tier"](#) to specify the ports to be used. This enables you to bypass automatic port configuration.

- a. Select **Specify Ports using a Configuration File**.
- b. In the file name field specify `ohs_ports.ini`.

- c. Click **Save**, then click **Next**.
- 5. On the Specify Security Updates screen, specify these values:
 - **Email Address:** The email address for your My Oracle Support account.
 - **Oracle Support Password:** The password for your My Oracle Support account.

Select: **I wish to receive security updates via My Oracle Support**.

Click **Next**.

- 6. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens.

Click **Configure**.

On the Configuration screen, the wizard launches multiple configuration assistants. This process can be lengthy. When it completes, click **Next**.

On the Installation Complete screen, click **Finish** to confirm your choice to exit.

7.4 Validating the Configuration

After the installation is completed, check that you can access the Oracle HTTP Server home page using the following URLs:

`http://WEBHOST1.mycompany.com:7777/`

`http://WEBHOST2.mycompany.com:7777/`

7.5 Configuring Virtual Hosts and Server Owner

To configure the virtual hosts complete the following tasks as described in this section.

- [Section 7.5.1, "Configuring Virtual Hosts"](#)
- [Section 7.5.2, "Configuring Oracle HTTP Server to Run as Software Owner"](#)
- [Section 7.5.3, "Update Oracle HTTP Server Runtime Parameters"](#)
- [Section 7.5.4, "Restarting the Oracle HTTP Servers"](#)
- [Section 7.5.5, "Validating the Configuration"](#)

7.5.1 Configuring Virtual Hosts

In order for Oracle Identity Management to work with the load balancer, you must create three virtual hosts.

To do so, create three separate files called `admin_vh.conf`, `oimadmin_vh.conf`, `sso_vh.conf`, and `idminternal_vh.conf` in `ORACLE_INSTANCE/config/OHS/component/moduleconf`.

On WEBHOST1 and WEBHOST2, add the following entries to the files:

Add to `admin_vh.conf`:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
    ServerName admin.mycompany.com:80
    RewriteEngine On
    RewriteOptions inherit
    RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
```

```
[R]
    RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_
url=/console" [R]
    ServerAdmin you@your.address
</VirtualHost>

Add to oimadmin_vh.conf (if using a split domain topology):

NameVirtualHost *:7777
<VirtualHost *:7777>
    ServerName oimadmin.mycompany.com:80
    RewriteEngine On
    RewriteOptions inherit
    RewriteRule ^/em/targetauth/emaslogout.jsp "/oamsso/logout.html?end_url=/em"
[R]
    RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_
url=/console" [R]
    ServerAdmin you@your.address
</VirtualHost>
```

Add to sso_vh.conf;

```
<VirtualHost *:7777>
    ServerName https://sso.mycompany.com:443
    RewriteEngine On
    RewriteOptions inherit
    UseCanonicalName On
</VirtualHost>
```

Add to idminternal_vh.conf:

```
<VirtualHost *:7777>
    ServerName http://idminternal.mycompany.com:80
    RewriteEngine On
    RewriteOptions inherit
    UseCanonicalName On
</VirtualHost>
```

7.5.2 Configuring Oracle HTTP Server to Run as Software Owner

By default, the Oracle HTTP server runs as the user `nobody`. In the Identity Management installation, the Oracle HTTP server should run as the Software owner and group.

To cause it to run as the appropriate user and group, edit the file `httpd.conf`, which is located in `ORACLE_INSTANCE/config/OHS/component_name`.

Find the section in `httpd.conf` where `User` is defined.

Change this section to read:

```
User User_who_installed_the_software
Group Group_under_which_the_HTTP_server_runs
```

Group is typically the default user group, for example: `oinstall`.

For example:

```
<IfModule !mpm_winnt_module>
#
# If you wish httpd to run as a different user or group, you must run
# httpd as root initially and it will switch.
```

```
#
# User/Group: The name (or #number) of the user/group to run httpd as.
# . On SCO (ODT 3) use "User nouser" and "Group nogroup".
# . On HP/UX you may not be able to use shared memory as nobody, and the
# suggested workaround is to create a user www and use that user.
# NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET)
# when the value of (unsigned)Group is above 60000;
# don't use Group #-1 on these systems!
#
User oracle
Group oinstall
</IfModule>
```

7.5.3 Update Oracle HTTP Server Runtime Parameters

By default, the Oracle HTTP Server contains parameter values that are suitable for most applications. These values, however, must be adjusted in IDM Deployments.

Proceed as follows:

Edit the file `httpd.conf`, which is located in:

```
ORACLE_INSTANCE/config/OHS/component_name
```

Find the entry that looks like this:

```
<IfModule mpm_worker_module>
```

Update the values in this section as follows:

```
<IfModule mpm_worker_module>
  ServerLimit 20
  StartServers 2
  MaxClients 1000
  MinSpareThreads 200
  MaxSpareThreads 800
  ThreadsPerChild 50
  MaxRequestsPerChild 10000
  AcceptMutex fcntl
  LockFile "${ORACLE_INSTANCE}/diagnostics/logs/${COMPONENT_TYPE}/${COMPONENT_
NAME}/http_lock"
</IfModule>
```

Save the file.

7.5.4 Restarting the Oracle HTTP Servers

Restart the Oracle HTTP Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

7.5.5 Validating the Configuration

Once the installation is completed check that it is possible to access the Oracle HTTP Server through the following URLs.

```
http://WEBHOST1.mycompany.com:7777/
```

```
http://WEBHOST2.mycompany.com:7777/
```

```
https://sso.mycompany.com/
```

```
http://idminternal.mycompany.com
```

7.6 Backing up the Web Tier Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

To back up the web tier installation, follow these steps,

1. Shut down the instance as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Back up the Middleware home on the web tier. On Linux, use the following command, as root:

```
tar -cvpf BACKUP_LOCATION/web.tar MW_HOME
```
3. Back up the Instance home on the web tier using the following command, as root:

```
tar -cvpf BACKUP_LOCATION/web_instance.tar ORACLE_INSTANCE
```
4. Start the instance as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

Note: Create backups on all machines in the web tier by following the steps shown.

For information about backing up the application tier configuration, see [Section 20.6, "Performing Backups and Recoveries."](#)

Creating Domains for an Enterprise Deployment

This chapter describes how to create a domain using the Configuration Wizard, Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. The topology you are creating dictates the number of domains you need to create. Once the initial domain has been created, it can be extended with other products as described later on in this book.

Note: Oracle strongly recommends that you read the release notes for any additional installation and deployment considerations prior to starting the setup process.

This chapter contains the following sections.

- [Section 8.1, "Overview of Creating a Domain"](#)
- [Section 8.2, "Choosing Single Domain or Split Domain"](#)
- [Section 8.3, "About Console URLs and Domains"](#)
- [Section 8.4, "Synchronize System Clocks"](#)
- [Section 8.5, "Enabling Virtual IP Addresses for Use by the Domain"](#)
- [Section 8.6, "Running the Configuration Wizard to Create a Domain with Oracle Access Manager, Oracle SOA Suite, and Oracle Identity Manager"](#)
- [Section 8.7, "Post-Configuration and Verification Tasks"](#)
- [Section 8.8, "Configuring Oracle HTTP Server for the WebLogic Domain"](#)
- [Section 8.9, "Manually Failing Over the WebLogic Administration Server"](#)
- [Section 8.10, "Backing Up the WebLogic Domain"](#)

8.1 Overview of Creating a Domain

[Table 8–1](#) lists the steps for creating a WebLogic domain, including post-configuration tasks.

Table 8–1 Steps for Creating a WebLogic Domain

Step	Description	More Information
Enabling a Virtual IP Address for Use by the Domain	Enable ADMINVHN or OIMADMINVHN on IDMHOST1 or OIMHOST1.	Section 8.5.1, "Enabling Virtual IP Addresses for Administration Servers"
Create a WebLogic Domain	Run the Configuration Wizard to create WebLogic domain.	Section 8.6, "Running the Configuration Wizard to Create a Domain with Oracle Access Manager, Oracle SOA Suite, and Oracle Identity Manager"
Post-Configuration and Verification Tasks	Follow the instructions for post-configuration and validation tasks.	Section 8.7, "Post-Configuration and Verification Tasks"
Configure the Oracle HTTP Server with the WebLogic domain	Configure the Oracle HTTP Server with the WebLogic domain and validate the configuration.	Section 8.8, "Configuring Oracle HTTP Server for the WebLogic Domain"
Back Up the Domain	Back up the newly configured WebLogic domain.	Section 8.10, "Backing Up the WebLogic Domain"

Once this domain is created and configured you can extend the domain to include other Identity Management components, as described in the next chapters.

8.2 Choosing Single Domain or Split Domain

Before starting to create your topology, you must determine whether to create a single domain topology, with all components in one domain, or creating a split domain topology, with Oracle Identity Manager in its own dedicated domain.

For a single domain topology, create one domain, IDMDomain.

For a split domain topology, you must create two domains. Specifically:

- A domain for most components, including directories, the HTTP server, Oracle Access Manager, Fusion Middleware Control, and WebLogic console. This is called IDMDomain.
- A domain for Oracle Identity Manager components, including OIM managed servers and separate WebLogic console and Fusion Middleware Control. This is called OIMDomain.

8.3 About Console URLs and Domains

The component URLs related to the domains in [Table 0–1](#), and the user names used to access them, are listed in the following two tables. [Table 8–2](#) lists the URLs available prior to web tier integration.

Table 8–2 URLs Available Prior to Web Tier Integration

Topology	Component	URL
IDMDomain	WebLogic Console	http://ADMINVHN.mycompany.com:7001/console
OIMDomain	WebLogic Console	http://OIMADMINVHN.mycompany.com:7001/console

After you have completed the tasks in [Section 8.8, "Configuring Oracle HTTP Server for the WebLogic Domain,"](#) the URLs listed in [Table 8–3](#) will be available.

Table 8–3 *URLs Available After Web Tier Integration*

Domain	Component	URL	User
IDMDomain	WebLogic Console	http://admin.mycompany.com/console	weblogic
IDMDomain	Fusion Middleware Control	http://admin.mycompany.com/em	weblogic
OIMDomain	WebLogic Console	http://oimadmin.mycompany.com/console	weblogic
OIMDomain	Fusion Middleware Control	http://oimadmin.mycompany.com/em	weblogic

8.4 Synchronize System Clocks

Oracle SOA uses Quartz to maintain its jobs and schedules in the database. Synchronize the system clocks for the SOA WebLogic cluster to enable proper functioning of jobs, adapters, and Oracle B2B.

8.5 Enabling Virtual IP Addresses for Use by the Domain

This section contains the following topics:

- [Section 8.5.1, "Enabling Virtual IP Addresses for Administration Servers"](#)

8.5.1 Enabling Virtual IP Addresses for Administration Servers

Note that this step is required for failover of the WebLogic Administration Server, regardless of whether other Oracle Fusion Middleware components are installed later or not.

You associate the Administration Server with a virtual IP address. This allows the Administration Server to be started on a different host if the primary host fails.

Check that the virtual host is enabled as follows:

Table 8–4 *Virtual Hosts for Single or Split Domain*

Domain	VIP	Enabled on Host
Single	ADMINVHN.mycompany.com.	IDMHOST1
Split	ADMINVHN.mycompany.com.	IDMHOST1
	OIMADMINVHN.mycompany.com.	OIMHOST1
Single and Split	OIMHOST1VHN.mycompany.com	OIMHOST1
	OIMHOST2VHN.mycompany.com	OIMHOST2
	SOAHOST1VHN.mycompany.com	OIMHOST1
	SOAHOST2VHN.mycompany.com	OIMHOST1

Note: This is the DNS name associated with the floating IP address. It is not the DNS name of the virtual host configured on the load balancer.

Linux

To enable the virtual IP address, run the following commands as root:

```
/sbin/ifconfig interface:index IPAddress netmask netmask
/sbin/arping -q -U -c 3 -I interface IPAddress
```

where *interface* is eth0, eth1, and so forth, and *index* is 0, 1, 2, and so forth.

For example:

```
/sbin/ifconfig eth0:1 100.200.140.206 netmask 255.255.255.0
```

Enable your network to register the new location of the virtual IP address:

```
/sbin/arping -q -U -c 3 -I eth0 100.200.140.206
```

Validate that the address is available by pinging it from another node, for example:

```
/bin/ping 100.200.140.206
```

Windows

To enable the virtual IP address, run the following command:

```
netsh interface ip add address interface IP_Address netmask
```

where *IP_Address* is the virtual IP address and the *netmask* is the associated netmask.

In the following example, the IP address is enabled on the interface Local Area Connection.

```
netsh interface ip add address "Local Area connection" 100.200.140.206
255.255.255.0
```

8.6 Running the Configuration Wizard to Create a Domain with Oracle Access Manager, Oracle SOA Suite, and Oracle Identity Manager

Run the Configuration Wizard from the Oracle common home directory to create a domain containing the Administration Server and managed servers. This domain supports Oracle Identity Manager and Oracle Access Manager. Later, you will extend the domain to contain other components.

If you are using a single domain topology, you run the Configuration Wizard once, on IDMHOST1, to create the IDMDomain.

If you are using a split domain topology, you must run the Configuration Wizard twice, to create two domains. You run it on IDMHOST1 when creating the IDMDomain and on OIMHOST1 when creating the OIMDomain.

Table 8–5 Domains to be Created

Topology	Name	Host	Listen Address
All	IDMDomain	IDMHOST1	ADMINVHN.mycompany.com
		OIMHOST1	OIMHOST1VHN.mycompany.com
		OIMHOST2	OIMHOST2VHN.mycompany.com
		OIMHOST1	SOAHOST1VHN.mycompany.com

Table 8–5 (Cont.) Domains to be Created

Topology	Name	Host	Listen Address
Split Domain	OIMDomain	OIMHOST1	SOAHOST2VHN.mycompany.com
		OIMHOST1	OIMADMINVHN.mycompany.com

As you proceed through the following steps, follow the procedures specified for the topology and domain that you are creating:

- Single domain topology, IDMDomain
- Split domain topology, IDMDomain
- Split domain topology, OIMDomain

To create IDMDomain and, optionally, OIMDomain, proceed as follows:

1. Ensure that the database where you installed the repository is running. For Oracle RAC databases, all instances should be running, so that the validation check later in the procedure is more reliable.
2. Change directory to the location of the Configuration Wizard. This is within the Oracle Common Home directory (created in [Chapter 6, "Installing the Software for an Enterprise Deployment"](#)).

```
cd ORACLE_BASE/product/fmw/oracle_common/common/bin
```

3. Start the Oracle Fusion Middleware Configuration Wizard

On Linux, type:

```
./config.sh
```

On Windows, type:

```
config.cmd
```

4. On the Welcome screen, select **Create a New WebLogic Domain**, and click **Next**.
5. On the Select Domain Source screen, do the following:
 - Select **Generate a domain configured automatically to support the following products**.
 - Select the following products for a single or split domain topology.

For single domain creation, select:

- **Oracle Identity Manager 11.1.1.3.0 [iam]**
- **Oracle SOA Suite - 11.1.1.0 [soa]**
- **Oracle Enterprise Manager [oracle_common]**
- **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [iam]**
- **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**
- **Oracle JRF [oracle_common]** (This should be selected automatically.)

For a split domain topology, when creating IDMDomain, select the following products:

- **Oracle Enterprise Manager [oracle_common]**

- **Oracle Access Manager with Database Policy Store - 11.1.1.3.0 [iam]**
IDMDomain only

- **Oracle JRF [oracle_common]** (This should be selected automatically.)

For a split domain topology, when creating OIMDomain, select the following products:

- **Oracle Identity Manager 11.1.1.3.0 [iam]** OIMDomain only
- **Oracle Enterprise Manager - 11.1.1.0 [iam]**
- **Oracle SOA Suite - 11.1.1.0 [soa]** OIMDomain only. This should be selected automatically.
- **Oracle JRF [oracle_common]** (This should be selected automatically.)
- **Oracle WSM Policy Manager - 11.1.1.0 [oracle_common]**

Click **Next**.

6. On the Specify Domain Name and Location screen, enter the domain name for the domain you are creating, either IDMDomain or OIMDomain.

Ensure that the domain directory matches the directory and shared storage mount point recommended in [Section 4.4.4, "Directory Structure."](#)

Enter

`ORACLE_BASE/admin/domain_name/aserver/`

for the domain directory and

`ORACLE_BASE/admin/domain_name/aserver/applications`

for the application directory, where *domain_name* is either IDMDomain or OIMDomain. The application directory should be in shared storage.

7. Click **Next**.

8. On the Configure Administrator Username and Password screen, enter the username (default is `weblogic`) and password to be used for the domain's administrator. For example:

- **Name:** `weblogic`
- **User Password:** *password for weblogic user*
- **Confirm User Password:** *password for weblogic user*
- **Description:** `This user is the default administrator.`

Click **Next**.

9. On the Configure Server Start Mode and JDK screen, do the following:
 - For WebLogic Domain Startup Mode, select **Production Mode**.
 - For JDK Selection, select **JRockit SDK**

Click **Next**.

10. On the Configure JDBC Component Schemas screen, select all the data sources listed on the page. The list will vary depending on whether you're setting up a single or a split domain.
 - **SOA Infrastructure**
 - **User Messaging Service**

- OIM MDS Schema
- OWSM MDS Schema
- SOA MDS Schema
- OAM Infrastructure
- OIM Schema

Under **RAC configuration for component schemas**, select **Convert to RAC multi data source**.

Click **Next**.

- 11.** On the **Configure RAC Multi Data Source Component Schema** page, select each of the schemas for your components, one by one. (Do not select schemas listed for previously configured components.) After you select a schema, enter its information into the appropriate fields, based on the following table:

Schema Name	Service Name	Host Names	Instance Names	Port	Schema Owner	Password
SOA Infrastructure	oimedg.mycompany.com	IDMDBHOST1-vip.mycompany.com	oimedg1	1521	EDG_SOAINFRA	password
		IDMDBHOST2-vip.mycompany.com	oimedg2	1521		
User Messaging Service	oimedg.mycompany.com	IDMDBHOST1-vip.mycompany.com	oimedg1	1521	EDG_ORASDPM	password
		IDMDBHOST2-vip.mycompany.com	oimedg2	1521		
OIM MDS Schema	oimedg.mycompany.com	IDMDBHOST1-vip.mycompany.com	oimedg1	1521	EDG_MDS	password
		IDMDBHOST2-vip.mycompany.com	oimedg2	1521		
OWSM MDS Schema	oimedg.mycompany.com	IDMDBHOST1-vip.mycompany.com	oimedg1	1521	EDG_MDS	password
		IDMDBHOST2-vip.mycompany.com	oimedg2	1521		
SOA MDS Schema	oimedg.mycompany.com	IDMDBHOST1-vip.mycompany.com	oimedg1	1521	EDG_MDS	password
		IDMDBHOST2-vip.mycompany.com	oimedg2	1521		
OIM Schema	oimedg.mycompany.com	IDMDBHOST1-vip.mycompany.com	oimedg1	1521	EDG_OIM	password

Schema Name	Service Name	Host Names	Instance Names	Port	Schema Owner	Password
		IDMDBHOST2-vip.mycompany.com	oimedg2	1521		

If you are using Oracle Database 11.2, replace the vip address and port with the 11.2 SCAN address and port.

Click **Next**.

12. On the Test JDBC Component Schema screen, the Configuration Wizard attempts to validate the data sources. If the data source validation succeeds, click **Next**. If it fails, click **Previous**, correct the problem, and try again.

Click **Next**.

13. On the Select Optional Configuration screen, select the following:

- **Administration Server**
- **JMS Distributed Destination** (required only on the domain that has OIM)
- **Managed Servers, Clusters and Machines**
- **JMS File Store** (required only on the domain that has OIM)

Click **Next**.

14. On the Configure the Administration Server screen, enter the following values:

- **Name:** AdminServer
- **Listen Address:**
ADMINVHN.mycompany.com (when creating IDMDomain).
OIMADMINVHN.mycompany.com (when creating OIMDomain)
- **Listen Port:** 7001
- **SSL listen port:** N/A
- **SSL enabled:** unchecked

Click **Next**.

15. When creating IDMDomain for a single domain topology or OIMDomain for a split domain topology, the next screen is the JMS Distributed Destination screen. This screen does not appear when you are creating IDMDomain for a split domain topology.

On the JMS Distributed Destination screen, ensure that all the JMS system resources listed on the screen are uniform distributed destinations. If they are not, select **UDD** from the drop down box. Ensure that the entries look like this:

JMS System Resource	Uniform/Weighted Distributed Destination
UMSJMSSystemResource	UDD
BPMJMSModule	UDD
SOAJMSModule	UDD
OIMJMSModule	UDD

Click **Next**.

An Override Warning box with the following message is displayed:

CFGFWK-40915: At least one JMS system resource has been selected for conversion to a Uniform Distributed Destination (UDD). This conversion will take place only if the JMS System resource is assigned to a cluster

Click **OK** on the Override Warning box.

16. The next screen is the Configure Managed Servers screen.

If you are creating IDMDomain for a single domain topology, when you first enter the Configure Managed Servers screen, three managed servers called oam_server1, oim_server1 and soa_server1 are created automatically. Rename oam_server to WLS_OAM1, soa_server1 to WLS_SOA1, and oim_server1 to WLS_OIM1 and update their attributes as shown in the following table.

Then, add three new managed servers called WLS_OAM2, WLS_OIM2 and WLS_SOA2 with the following attributes.

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_OAM1	IDMHOST1	14100	N/A	No
WLS_OAM2	IDMHOST2	14100	N/A	No
WLS_SOA1	SOAHOST1VHN	8001	N/A	No
WLS_SOA2	SOAHOST2VHN	8001	N/A	No
WLS_OIM1	OIMHOST1VHN	14000	N/A	No
WLS_OIM2	OIMHOST2VHN	14000	N/A	No

Leave all the other fields at the default settings.

When you are creating a split domain topology, during creation of IDMDomain, one managed server, oam_server1, is created automatically. Change it to WLS_OAM1 and update its attributes as shown in the table. Also create WLS_OAM2 with the attributes shown in the table.

During creation of OIMDomain, only two managed servers, oim_server1 and soa_server1 are created automatically. Change them to WLS_OIM1 and WLS_SOA1, respectively, and update their attributes as shown in the table. Also add WLS_OIM2 and WLS_SOA2, with the attributes shown in the table.

Notes:

- Do not change the configuration of the managed servers that were configured as a part of previous deployments.
 - Do not delete the default managed servers that are created. Rename them as described.
-

17. The next screen is the Configure Clusters screen.

Create clusters by clicking **Add**. The clusters you create depend on the topology, as shown in [Table 8–6](#).

Table 8–6 Clusters

Topology	Domain	Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
Single Domain	IDMDomain	oam_cluster	unicast	n/a	n/a	
	IDMDomain	oim_cluster	unicast	n/a	n/a	
	IDMDomain	soa_cluster	unicast	n/a	n/a	SOAHOST1V HN:8001,SOA HOST2VHN:8 001
Split Domain	IDMDomain	oam_cluster	unicast	n/a	n/a	
	OIMDomain	oim_cluster	unicast	n/a	n/a	
	OIMDomain	soa_cluster	unicast	n/a	n/a	SOAHOST1V HN:8001,SOA HOST2VHN:8 001

Note: Do not change the configuration of the clusters that were configured as a part of previous deployments.

18. On the Assign Servers to Clusters screen, associate the managed servers with the cluster. Click the cluster name in the right pane. Click the managed server under **Servers**, then click the arrow to assign it to the cluster.

Table 8–7 Servers to Assign to Clusters

Cluster	Server
oam_cluster	WLS_OAM1
	WLS_OAM2
oim_cluster	WLS_OIM1
	WLS_OIM2
soa_cluster	WLS_SOA1
	WLS_SOA2

Click **Next**.

Note: Do not make any changes to clusters that already have entries defined.

19. On the Configure Machines screen, click the **Unix Machine** tab (**Machines** tab on Windows) and then click **Add** to add the following machine. The machine name does not need to be a valid host name or listen address, it is just a unique identifier of a node manager location.

Then create a machine for each host in the topology

- a. **Name:** Name of the host. Best practice is to use the DNS name.
- b. **Node Manager Listen Address:** DNS name of the machine.

c. Node Manager Port: Port for Node Manager

Provide the information shown in the following table.

If you are creating IDMDomain for a single domain topology, create all the hosts shown in the table.

If you are creating IDMDomain for a split domain topology, create IDMHOST1, IDMHOST2, and ADMINHOST.

If you are creating OIMDomain for a split domain topology, create OIMHOST1, OIMHOST2, and OIMADMINHOST.

Name	Node Manager Listen Address	Node Manager Listen Port
OIMHOST1	OIMHOST1	5556
OIMHOST2	OIMHOST2	5556
IDMHOST1	IDMHOST1	5556
IDMHOST2	IDMHOST2	5556
ADMINHOST	LOCALHOST	5556

Leave the default values for all other fields.

Delete the default local machine entry under the **Machines** tab.

Click **Next**.

20. Click **Next**.**21.** On the Assign Servers to Machines screen, assign servers to machines as follows:

- **ADMINHOST:** AdminServer
- **OIMADMINHOST:** AdminServer
- **OIMHOST1:** WLS_OIM1, WLS_SOA1
- **OIMHOST2:** WLS_OIM2, WLS_SOA2
- **IDMHOST1:** WLS_OAM1
- **IDMHOST2:** WLS_OAM2

If you are creating IDMDomain for a single domain deployment, the following hosts appear.

- **ADMINHOST:** AdminServer
- **OIMHOST1:** WLS_OIM1, WLS_SOA1
- **OIMHOST2:** WLS_OIM2, WLS_SOA2
- **IDMHOST1:** WLS_OAM1
- **IDMHOST2:** WLS_OAM2

If you are creating IDMDomain for a split domain deployment, ADMINHOST, IDMHOST1 and IDMHOST2 appear.

If you are creating OIMDomain for a split domain deployment, OIMADMINHOST, OIMHOST1, and OIMHOST2 appear.

Click **Next** to continue.

22. If you are creating OIMDomain for a split domain deployment, the Configure JMS File Stores screen appears. On the Configure JMS File Stores screen, update the directory locations for the JMS file stores. Provide the following information.

Name	Directory
UMSJMSFileStore_auto_1	/u01/app/oracle/admin/ <i>domain_name</i> /soa_cluster/jms/UMSJMSFileStore_auto_1
UMSJMSFileStore_auto_2	/u01/app/oracle/admin/ <i>domain_name</i> /soa_cluster/jms/UMSJMSFileStore_auto_2
BPMJMSServer_auto_1	/u01/app/oracle/admin/ <i>domain_name</i> /soa_cluster/jms/BPMJMSServer_auto_1
BPMJMSServer_auto_2	/u01/app/oracle/admin/ <i>domain_name</i> /soa_cluster/jms/BPMJMSServer_auto_2
SOAJMSFileStore_auto_1	/u01/app/oracle/admin/ <i>domain_name</i> /soa_cluster/jms/SOAJMSFileStore_auto_1
SOAJMSFileStore_auto_2	/u01/app/oracle/admin/ <i>domain_name</i> /soa_cluster/jms/SOAJMSFileStore_auto_2
OIMJMSFileStore_auto_1	/u01/app/oracle/admin/ <i>domain_name</i> /oim_cluster/jms/OIMJMSFileStore_auto_1
OIMJMSFileStore_auto_2	/u01/app/oracle/admin/ <i>domain_name</i> /oim_cluster/jms/OIMJMSFileStore_auto_2

If you are creating IDMDomain for a split domain deployment, the Configure JMS File Stores screen does not appear.

Click **Next**.

Notes:

- Use /u01/app/oracle/admin/*IDMDomain*/soa_cluster/jms/ as the directory location for the UMSJMSFileStore_auto_1, UMSJMSFileStore_auto_2, BPMJMSServer_auto_1, BPMJMSServer_auto_2, SOAJMSFileStore_auto_1, and SOAJMSFileStore_auto_2 JMS file stores
 - Use /u01/app/oracle/admin/*IDMDomain*/oim_cluster/jms/ as the directory location for the OIMJMSFileStore_auto_1 and OIMJMSFileStore_auto_2 JMS file stores
 - The locations /u01/app/oracle/admin/*IDMDomain*/soa_cluster/jms/ and /u01/app/oracle/admin/*IDMDomain*/oim_cluster/jms/ are on shared storage and must be accessible from OIMHOST1 and OIMHOST2
-
-

23. On the Configuration Summary screen, validate that your choices are correct, then click **Create**.

24. On the Create Domain screen, click **Done**.

8.7 Post-Configuration and Verification Tasks

After configuring the domain with the configuration Wizard, follow these instructions for post-configuration and verification.

This section includes the following topics:

- [Section 8.7.1, "Creating boot.properties for the WebLogic Administration Server on IDMHOST1"](#)
- [Section 8.7.2, "Creating boot.properties for the WebLogic Administration Server on OIMHOST1"](#)
- [Section 8.7.3, "Starting Node Manager"](#)
- [Section 8.7.4, "Updating the Node Manager Credentials"](#)
- [Section 8.7.5, "Validating the WebLogic Administration Server"](#)
- [Section 8.7.6, "Removing IDM Domain Agent on IDMHOST1"](#)
- [Section 8.7.7, "Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server"](#)
- [Section 8.7.8, "Propagate Changes to Remote Servers"](#)
- [Section 8.7.10, "Start Node Manager on Remote Hosts"](#)
- [Section 8.7.11, "Disabling Host Name Verification for the Oracle WebLogic Administration Server"](#)
- [Section 8.7.12, "Stopping and Starting the WebLogic Administration Server"](#)

8.7.1 Creating boot.properties for the WebLogic Administration Server on IDMHOST1

Create a `boot.properties` file for the Administration Server on IDMHOST1. If the file already exists, edit it. The `boot.properties` file enables the Administration Server to start without prompting you for the administrator username and password.

For the Administration Server:

1. Create the following directory structure.

```
mkdir -p ORACLE_
BASE/admin/IDMDomain/aserver/IDMDomain/servers/AdminServer/security
```

2. In a text editor, create a file called `boot.properties` in the last directory created in the previous step, and enter the username and password in the file. For example:

```
username=weblogic
password=password for weblogic user
```

3. Save the file and close the editor.

Note: The username and password entries in the file are not encrypted until you start the Administration Server, as described in [Section 8.7.4, "Updating the Node Manager Credentials."](#) For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, start the server as soon as possible so that the entries are encrypted.

8.7.2 Creating boot.properties for the WebLogic Administration Server on OIMHOST1

If you are using a split domain topology, create a `boot.properties` file for the Administration Server on OIMHOST1. If the file already exists, edit it. The `boot.properties` file enables the Administration Server to start without prompting you for the administrator username and password.

For the Administration Server:

1. Create the following directory structure.

```
mkdir -p ORACLE_  
BASE/admin/OIMDomain/aserver/OIMDomain/servers/AdminServer/security
```

2. In a text editor, create a file called `boot.properties` in the last directory created in the previous step, and enter the username and password in the file. For example:

```
username=weblogic  
password=password for weblogic user
```

3. Save the file and close the editor.

Note: The username and password entries in the file are not encrypted until you start the Administration Server, as described in [Section 8.7.4, "Updating the Node Manager Credentials."](#) For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, start the server as soon as possible so that the entries are encrypted.

8.7.3 Starting Node Manager

Perform these steps to start Node Manager on the administration host:

1. Run the `startNodeManager.sh` script located under the `ORACLE_
BASE/product/fmw/wlserver_10.3/server/bin/` directory.
2. Run the `setNMProps.sh` script to set the `StartScriptEnabled` property to `true`:

```
cd MW_HOME/oracle_common/common/bin  
./setNMProps.sh
```

Note: You must use the `StartScriptEnabled` property to avoid class loading failures and other problems.

3. Stop the Node Manager by killing the Node Manager process, or stop the service in Windows.
4. Start Node Manager for the Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

8.7.4 Updating the Node Manager Credentials

You start the Administration server by using WLST and connecting to Node Manager. The first start of the Administration Server with Node Manager, however, requires that you change the default username and password that the Configuration Wizard sets for Node Manager. Therefore you must use the start script for the Administration

Server for the first start. Follow these steps to start the Administration Server using Node Manager.

Steps 1-4 are required for the first start operation, but subsequent starts require only Step 4.

1. Start the Administration Server using the start script in the domain directory.

```
cd ORACLE_BASE/admin/domain_name/aserver/domain_name/bin
./startWebLogic.sh
```

2. Use the Administration Console to update the Node Manager credentials on IDMDomain.

- a. In a browser, go to the listen address for the domain, as listed in [Table 8-5](#). For example:

```
http://ADMINVHN.mycompany.com:7001/console.
```

- b. Log in as the administrator.
- c. Click **Lock and Edit**.
- d. Click *domain_name*.
- e. Select **Security** tab then **General** tab.
- f. Expand **Advanced Options**.
- g. Enter a new username for Node Manager or make a note of the existing one and update the Node Manager password.
- h. Click **Save**.
- i. Click **Activate Changes**.

Update the Node Manager credentials on the domain. Go to the listen address for the other domains, as listed in [Table 8-5](#), and perform the same steps.

3. Stop the WebLogic Administration Server by issuing the command `stopWebLogic.sh` located under the `ORACLE_BASE/admin/domain_name/aserver/domain_name/bin` directory.
4. Start WLST and connect to the Node Manager with `nmconnect` and the credentials you just updated. Then start the WebLogic Administration Server using `nmStart`.

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

On Windows, the command is:

```
wlst.cmd
```

Once in the WLST shell, execute the following commands:

```
nmConnect('Admin_User', 'Admin_Password', 'ADMINHOST1', '5556',
  domain_name, 'ASERVER_HOME/domain_name')
nmStart('AdminServer')
```

where *domain_name* is the name of the domain, *Admin_user* and *Admin_Password* are the Node Manager username and password you entered in Step 2. For example:

```
nmConnect('weblogic', 'password', 'OAMHOST1', '5556',
  'IDMDomain', '/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain')
```

```
nmStart('AdminServer')
```

8.7.5 Validating the WebLogic Administration Server

Perform these steps to ensure that the Administration Server is properly configured:

1. In a browser, go to the Oracle WebLogic Server Administration Console at the URL listed in [Table 8–2](#), for example:
`http://ADMINVHN.mycompany.com:7001/console`
2. Log in as the WebLogic administrator, for example: `weblogic`.
3. Check that you can access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`.
4. Log in to Oracle Enterprise Manager Fusion Middleware Control as the WebLogic administrator, for example: `weblogic`.

If you are using a split domain topology, perform these steps as well:

1. In a browser, go to `http://OIMADMINVHN.mycompany.com:7001/console`.
2. Log in as the WebLogic administrator, for example: `weblogic`.
3. Check that you can access Oracle Enterprise Manager Fusion Middleware Control at `http://OIMADMINVHN.mycompany.com:7001/em`.
4. Log in to Oracle Enterprise Manager Fusion Middleware Control as the WebLogic administrator, for example: `weblogic`.

8.7.6 Removing IDM Domain Agent on IDMHOST1

By default, the IDMDomain Agent provides single sign-on capability for administration consoles. In enterprise deployments, WebGate handles single sign-on, so you must remove the IDMDomain agent. Remove the IDMDomain Agent as follows:

Log in to the WebLogic console at the URL listed in [Table 8–2](#).

Then:

1. Select **Security Realms** from the **Domain Structure** Menu
2. Click **myrealm**.
3. Click the **Providers** tab.
4. Click **Lock and Edit** from the **Change Center**.
5. In the list of authentication providers, select **IAMSuiteAgent**.
6. Click **Delete**.
7. Click **Yes** to confirm the deletion.
8. Click **Activate Changes** from the **Change Center**.
9. Restart WebLogic Administration Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

8.7.7 Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server

Use the `pack` and `unpack` commands to separate the domain directory used by the Administration Server from the domain directory used by the managed server in `IDMHOST1`, as recommended in [Chapter 4, "Preparing the File System for an Enterprise Deployment."](#) If you are using a split domain topology, also use the `pack` and `unpack` commands on `OIMHOST`.

Before running the `unpack` script, be sure the following directory exists as explained in [Chapter 4.4, "About Recommended Locations for the Different Directories."](#)

```
ORACLE_BASE/admin/domain_name/mserver
```

To create a separate domain directory on `IDMHOST1`:

1. Run the `pack` command to create a template pack as follows:

```
cd ORACLE_COMMON_HOME/common/bin
```

```
./pack.sh -managed=true -domain=ORACLE_BASE/admin/domain_name/aserver/domain_name -template=domaintemplate.jar -template_name=domain_template
```

2. Run the `unpack` command to unpack the template in the managed server domain directory as follows:

```
cd ORACLE_COMMON_HOME/common/bin
```

```
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name -template=domaintemplate.jar -app_dir=ORACLE_BASE/admin/domain_name/mserver/applications
```

If you are using a split domain topology, also perform Steps 1 and 2 on `OIMHOST1`.

Note: You must have write permissions on the following directory before running the `unpack` command:

```
/ORACLE_BASE/admin/domain_name
```

For example:

```
ORACLE_BASE/admin/IDMDomain/
```

Note: The configuration steps provided in this enterprise deployment topology are documented with the assumption that a local (per node) domain directory is used for each managed server.

8.7.8 Propagate Changes to Remote Servers

Before you can start managed servers on remote hosts, you must first perform an `unpack` on those servers. Proceed as follows.

Single Domain

Using the file `domaintemplate.jar` created in [Section 8.7.7, "Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration"](#)

[Server](#)," perform an unpack on the hosts: IDMHOST2, OIMHOST1 and OIMHOST2 by using the following commands:

```
cd ORACLE_COMMON_HOME/common/bin
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_
name-template=domaintemplate.jar -app_dir=ORACLE_BASE/admin/domain_
name/mserver/applications
```

Split Domain

Using the file `domaintemplate.jar` created for the domain IDMDomain in [Section 8.7.7, "Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server](#)," perform an unpack on the host IDMHOST2 by using the following commands:

```
cd ORACLE_COMMON_HOME/common/bin
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_
name-template=domaintemplate.jar -app_dir=ORACLE_BASE/admin/domain_
name/mserver/applications
```

Using the file `domaintemplate.jar` created for the domain OIMDomain in [Section 8.7.7, "Creating a Separate Domain Directory for Managed Servers in the Same Node as the Administration Server](#)," perform an unpack on the host OIMHOST2 by using the following commands:

```
cd ORACLE_COMMON_HOME/common/bin
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_
name-template=domaintemplate.jar -app_dir=ORACLE_BASE/admin/domain_
name/mserver/applications
```

8.7.9 Copy SOA Composites to Managed Server Directory

When SOA first starts, it automatically deploys a number of applications that are located in the `DOMAIN_HOME/soa` directory. Performing pack and unpack does not populate this directory, so you must create it manually.

Single Domain

Copy the `soa` directory from `ASERVER_HOME/IDMDomain/soa` to `MSERVER_HOME/IDMDomain` on OIMHOST1 and OIMHOST2.

For example:

```
scp -rp /u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/soa
user@OIMHOST1:/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain/soa
```

Split Domain

Copy the `soa` directory from `ASERVER_HOME/OIMDomain/soa` to `MSERVER_HOME/OIMDomain`

For example:

```
cp -rp /u01/app/oracle/admin/OIMDomain/aserver/OIMDomain/soa
/u01/app/oracle/admin/OIMDomain/mserver/OIMDomain/soa
```

8.7.10 Start Node Manager on Remote Hosts

Perform this step on the following hosts:

Single Domain: IDMHOST2, OIMHOST1, OIMHOST2

Split Domain: IDMHOST2, OIMHOST2

If the Node Manager is not already started, perform the following steps to start it:

Start the Node Manager to create the `nodemanager.properties` file by using the `startNodemanager.sh` script located under the `MW_HOME/wlserver_10.3/server/bin` directory.

Before you can start the Managed Servers by using the console, node manager requires that you set the property `StartScriptEnabled` to `true`. You set it by running the `setNMProps.sh` script located under the `MW_HOME/oracle_common/common/bin` directory, as follows.

```
cd MW_HOME/oracle_common/common/bin
./setNMProps.sh
```

Stop and Start the Node Manager as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components"](#) so that the properties take effect.

8.7.11 Disabling Host Name Verification for the Oracle WebLogic Administration Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server. (See [Chapter 16, "Setting Up Node Manager for an Enterprise Deployment."](#)) If you have not configured the server certificates, you will receive errors when managing the different WebLogic Servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the EDG topology configuration is complete as described in [Chapter 16, "Setting Up Node Manager for an Enterprise Deployment."](#)

Perform these steps to disable host name verification:

1. Go to the Oracle WebLogic Server Administration Console at the URL listed in [Table 8–2](#).
2. Log in as the user `weblogic`, using the password you specified during the installation.
3. Click **Lock and Edit**.
4. Expand the Environment node in the Domain Structure window.
5. Click **Servers**. The Summary of Servers page appears.
6. Select **AdminServer(admin)** in the **Name** column of the table. The Settings page for AdminServer(admin) appears.
7. Click the **SSL** tab.
8. Click **Advanced**.
9. Set Hostname Verification to **None**.
10. Click **Save**.
11. Click **Activate Changes**.

8.7.12 Stopping and Starting the WebLogic Administration Server

1. Stop the Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components"](#)
2. Start WLST and connect to the Node Manager with `nmconnect` and the credentials set previously described. Then start the Administration Server using `nmStart`.

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

Once in the WLST shell, execute the following commands:

IDMDomain

```
nmConnect('Admin_User','Admin_Pasword','IDMHOST1','5556',
          'IDMDomain','/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain')
nmStart('AdminServer')
```

OIMDomain

```
nmConnect('Admin_User','Admin_Pasword','OIMHOST1','5556',
          'OIMDomain','/u01/app/oracle/admin/OIMDomain/aserver/OIMDomain')
nmStart('AdminServer')
```

where *Admin_user* and *Admin_Password* are the Node Manager username and password you entered in Step 2 of [Section 8.7.4, "Updating the Node Manager Credentials."](#)

Note: *Admin_user* and *Admin_Password* are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the *ORACLE_BASE/admin/domain_name/aserver/domain_name/config/nodemanager/nm_password.properties* file.

8.8 Configuring Oracle HTTP Server for the WebLogic Domain

This section describes tasks for configuring Oracle HTTP Server for the WebLogic Domain, and for verifying the configuration.

This section includes the following topics:

- [Section 8.8.1, "Configuring Oracle HTTP Server for the WebLogic Administration Server"](#)
- [Section 8.8.2, "Configuring Oracle HTTP Server for the Oracle Identity Manager Domain"](#)
- [Section 8.8.3, "Restart Oracle HTTP Server"](#)
- [Section 8.8.4, "Registering Oracle HTTP Server with WebLogic Server"](#)
- [Section 8.8.5, "Setting the Front End URL for the Administration Console"](#)
- [Section 8.8.6, "Enabling WebLogic Plug-in"](#)
- [Section 8.8.7, "Validating Access to Domains"](#)

8.8.1 Configuring Oracle HTTP Server for the WebLogic Administration Server

To enable Oracle HTTP Server to route to the Administration Server, you must set the the corresponding mount points in your HTTP Server configuration.

On each of the web servers on WEBHOST1 and WEBHOST2 edit the file *admin_vh.conf*, which you created in [Section 7.5.1, "Configuring Virtual Hosts."](#) The file is the directory:

```
ORACLE_INSTANCE/config/OHS/component/moduleconf
```


Add the following new entries within the VirtualHost directive, as shown:

```
NameVirtualHost *:7777

<VirtualHost *:7777>

    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    ...

    # Admin Server and EM
    <Location /console>
        SetHandler weblogic-handler
        WebLogicHost ADMINVHN.mycompany.com
        WeblogicPort 7001
    </Location>

    <Location /consolehelp>
        SetHandler weblogic-handler
        WebLogicHost ADMINVHN.mycompany.com
        WeblogicPort 7001
    </Location>

    <Location /em>
        SetHandler weblogic-handler
        WebLogicHost ADMINVHN.mycompany.com
        WeblogicPort 7001
    </Location>

</VirtualHost>
```

Notes:

- Values such as `admin.mycompany:80` and `you@youraddress` that are noted in this document serve as examples only. Enter values based on the actual environment.
 - If you are not using a virtual host for your Administration Server host (single instance), replace `ADMINVHN.mycompany.com` with `IDMHOST1.mycompany.com`.
-

8.8.2 Configuring Oracle HTTP Server for the Oracle Identity Manager Domain

If you are placing your Oracle Identity Manager components into a separate domain, you must add a separate virtual host configuration into your Oracle HTTP Server configuration as follows:

On each of the web servers on WEBHOST1 and WEBHOST2, edit the file `oimadmin_vh.conf` in the directory:

`ORACLE_INSTANCE/config/OHS/component/moduleconf`

Add the lines in bold within the VirtualHost directive, as shown:

```
<VirtualHost *:7777>

    ServerName oimadmin.mycompany.com:80
    ServerAdmin you@your.address
    ...
```

```
# Admin Server and EM
<Location /console>
    SetHandler weblogic-handler
    WebLogicHost OIMADMINVHN.mycompany.com
    WeblogicPort 7001
</Location>

<Location /consolehelp>
    SetHandler weblogic-handler
    WebLogicHost OIMADMINVHN.mycompany.com
    WeblogicPort 7001
</Location>

<Location /em>
    SetHandler weblogic-handler
    WebLogicHost OIMADMINVHN.mycompany.com
    WeblogicPort 7001
</Location>

</VirtualHost>
```

Note: Values such as `oimadmin.mycompany:80` and `you@youraddress` that are noted in this document serve as examples only. Enter values based on the actual environment.

8.8.3 Restart Oracle HTTP Server

Restart OHS on WEBHOST1 as follows:

```
ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc ias-component=ohs1
```

Restart OHS on WEBHOST2:

```
ORACLE_BASE/admin/instance_name/bin/opmnctl restartproc ias-component=ohs2
```

8.8.4 Registering Oracle HTTP Server with WebLogic Server

For Oracle Enterprise Manager Fusion Middleware Control to be able to manage and monitor the Oracle HTTP server, you must register the Oracle HTTP server with IDMDomain. Even when using a split domain topology, register the Oracle HTTP Server with IDMDomain only. To do this, you must register Oracle HTTP Server with WebLogic Server using the following command:

```
cd ORACLE_BASE/admin/instance_name/bin
./opmnctl registerinstance -adminHost ADMINVHN.mycompany.com \
    -adminPort 7001 -adminUsername weblogic
```

You must also run this command from WEBHOST2 for ohs2.

8.8.5 Setting the Front End URL for the Administration Console

Oracle WebLogic Server Administration Console tracks changes that are made to ports, channels and security using the console. When changes made through the console are activated, the console validates its current listen address, port and protocol. If the listen address, port and protocol are still valid, the console redirects the

HTTP request, replacing the host and port information with the Administration Server's listen address and port. When the Administration Console is accessed using a load balancer, you must change the Administration Server's front end URL so that the user's browser is redirected to the appropriate load balancer address. To make this change, perform the following steps:

1. Log in to Oracle WebLogic Server Administration Console at the URL listed in [Table 8–2](#), for example:

```
http://ADMINVHN.mycompany.com:7001/console
```

2. Click **Lock and Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers** to open the Summary of Servers page.
5. Select **Admin Server** in the Names column of the table. The Settings page for AdminServer(admin) appears.
6. Click the **Protocols** tab.
7. Click the **HTTP** tab.
8. Set the **Front End Host** field to your load balancer address, `admin.mycompany.com` for IDMDomain or `oimadmin.mycompany.com` for OIMDomain in a split domain topology.
9. Set **FrontEnd HTTP Port** to 80
10. Save and activate the changes.

To eliminate redirections, best practice is to disable the Administration console's **Follow changes** feature. To do this, log in to the administration console and click **Preferences->Shared Preferences**. Deselect **Follow Configuration Changes** and click **Save**.

8.8.6 Enabling WebLogic Plug-in

In Enterprise deployments, Oracle WebLogic Server is fronted by Oracle HTTP servers. The HTTP servers are, in turn, fronted by a load balancer, which performs SSL translation. In order for internal loopback URLs to be generated with the `https` prefix, Oracle WebLogic Server must be informed that it receives requests through the Oracle HTTP Server WebLogic plug-in.

The plug-in can be set at either the domain, cluster, or Managed Server level. Because all requests to Oracle WebLogic Server are through the Oracle OHS plug-in, set it at the domain level.

To do this perform the following steps:

1. Log in to the Oracle WebLogic Server Administration Console at the URL listed in [Table 8–2](#).
2. Click **Lock and Edit**.
3. Click **IDMDomain** in the Domain Structure Menu.
4. Click the **Configuration** tab.
5. Click the **Web Applications** sub tab.
6. Select **WebLogic Plugin Enabled**.
7. Click **Save and Activate the Changes**.

8. Restart WebLogic Administration Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

If you are using a split domain topology, also log in to the Oracle WebLogic Server Administration Console at

`http://OIMADMINVHN.mycompany.com:7001/console` and perform the same steps. In Step 3, click **OIMDOMAIN** in the Domain Structure Menu.

8.8.7 Validating Access to Domains

Verify that the server status is reported as **Running** in the Administration Console. If the server is shown as **Starting** or **Resuming**, wait for the server status to change to **Started**. If another status is reported (such as **Admin** or **Failed**), check the server output log files for errors. See [Section 20.9, "Troubleshooting"](#) for possible causes.

Validate Administration Console and Oracle Enterprise Manager Fusion Middleware Control through Oracle HTTP Server using each of the `console` and `em` URLs in [Table 8–3, "URLs Available After Web Tier Integration"](#).

For information on configuring system access through the load balancer, see [Section 3.3, "Configuring the Load Balancers."](#)

Note: After registering the Oracle HTTP Server as described in [Section 8.8.4, "Registering Oracle HTTP Server with WebLogic Server,"](#) the Oracle HTTP Server should appear as a manageable target in Oracle Enterprise Manager Fusion Middleware Control. To verify this, log in to Fusion Middleware Control. The **WebTier** item in the navigation tree should show that Oracle HTTP Server has been registered.

8.9 Manually Failing Over the WebLogic Administration Server

This section discusses how to fail over the Administration Server to **IDMHOST2** and how to fail it back to **IDMHOST1**.

If you are using a split domain topology, follow the same procedures to fail over the Administration Server to **OIMHOST2** and how to fail it back to **OIMHOST1**.

This section contains the following topics:

- [Section 8.9.1, "Failing over the Administration Server to IDMHOST2"](#)
- [Section 8.9.2, "Starting the Administration Server on IDMHOST2"](#)
- [Section 8.9.3, "Validating Access to IDMHOST2 Through Oracle HTTP Server"](#)
- [Section 8.9.4, "Failing the Administration Server Back to IDMHOST1"](#)

8.9.1 Failing over the Administration Server to IDMHOST2

If a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from **IDMHOST1** to **IDMHOST2**.

If you are using a split domain topology, follow the same procedures to fail over the Administration Server from **OIMHOST1** to **OIMHOST2**.

Assumptions:

- The Administration Server is configured to listen on ADMINVHN.mycompany.com, and not on ANY address. See step 10 in [Section 8.6, "Running the Configuration Wizard to Create a Domain with Oracle Access Manager, Oracle SOA Suite, and Oracle Identity Manager."](#)
- The Administration Server is failed over from IDMHOST1 to IDMHOST2, and the two nodes have these IP addresses:
 - IDMHOST1: 100.200.140.165
 - IDMHOST2: 100.200.140.205
 - ADMINVIP: 100.200.140.206

This is the Virtual IP address where the Administration Server is running, assigned to *interface:index* (for example, eth1:2), available in IDMHOST1 and IDMHOST2.
- The domain directory where the Administration Server is running in IDMHOST1 is on a shared storage and is mounted also from IDMHOST2.

Note: NM in IDMHOST2 does not control the domain at this point, since `unpack/nmEnroll` has not been run yet on IDMHOST2. But for the purpose of AdminServer failover and control of the AdminServer itself, Node Manager is fully functional

- Oracle WebLogic Server and Oracle Fusion Middleware Components have been installed in IDMHOST2 as described in previous chapters. That is, the same path for `IDM_ORACLE_HOME` and `MW_HOME` that exists in IDMHOST1 is available in IDMHOST2.

The following procedure shows how to fail over the Administration Server to a different node, IDMHOST2.

Linux

1. Stop the Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Migrate the IP address to the second node.
 - a. Run the following command as root on IDMHOST1 (where *x:y* is the current interface used by ADMINVHN.mycompany.com):

```
/sbin/ifconfig x:y down
```

For example:

```
/sbin/ifconfig eth0:1 down
```

- b. Run the following command on IDMHOST2:

```
/sbin/ifconfig interface:index IP_Address netmask netmask
```

For example:

```
/sbin/ifconfig eth0:1 10.0.0.1 netmask 255.255.255.0
```

Note: Ensure that the netmask and interface to be used match the available network configuration in IDMHOST2.

3. Update routing tables by using arping, for example:

```
/sbin/arping -b -A -c 3 -I eth0 10.0.0.1
```

Windows

1. Stop the Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Migrate the IP address to the second node.

- a. Run the following command as root on IDMHOST1

```
netsh interface ip delete address interface netmask
```

In the following example, the IP address is disabled on the interface Local Area Connection:

```
netsh interface ip delete address "Local Area connection" 100.200.140.206
```

- b. Run the following command on IDMHOST2:

```
netsh interface ip add address interface IP_Address netmask
```

In the following example, the IP address is enabled on the interface Local Area Connection:

```
netsh interface ip add address "Local Area connection" 100.200.140.206  
255.255.255.0
```

8.9.2 Starting the Administration Server on IDMHOST2

Perform the following steps to start Node Manager on IDMHOST2.

If you are using a split domain topology, follow the same procedures to start the Node Manager on OIMHOST2.

1. On IDMHOST1, unmount the Administration Server domain directory. For example:

```
umount /u01/app/oracle/admin/IDMDomain/aserver/
```

2. On IDMHOST2, mount the Administration Server domain directory. For example:

```
mount /u01/app/oracle/admin/IDMDomain/aserver/
```

3. Start Node Manager by using the following commands:

```
cd ORACLE_BASE/product/fmw/wlserver_10.3/server/bin  
./startNodeManager.sh
```

4. Stop the Node Manager by killing the Node Manager process, or stop the service in Windows.

Note: Starting and stopping Node Manager at this point is only necessary the first time you run Node Manager. Starting and stopping it creates a property file from a predefined template. The next step adds properties to that property file.

5. Run the `setNMProps.sh` script to set the `StartScriptEnabled` property to `true` before starting Node Manager:

```
cd $MW_HOME/oracle_common/common/bin
./setNMProps.sh
```

Note: You must use the `StartScriptEnabled` property to avoid class loading failures and other problems.

6. Start the Node Manager as described in [Section 20.1.5.3, "Starting Node Manager for an Administration Server."](#)
7. Start the Administration Server on `IDMHOST2`.

```
cd $ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

Once in the WLST shell, execute the following commands:

```
nmConnect('Admin_User','Admin_Password', 'IDMHOST2','5556',
'IDMDomain','/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain')
nmStart('AdminServer')
```

8. Test that you can access the Administration Server on `IDMHOST2` as follows:
 - a. Ensure that you can access the Oracle WebLogic Server Administration Console at:

```
http://ADMINVHN.mycompany.com:7001/console.
```
 - b. Check that you can access and verify the status of components in the Oracle Enterprise Manager at: `http://ADMINVHN.mycompany.com:7001/em`.

8.9.3 Validating Access to IDMHOST2 Through Oracle HTTP Server

Perform the same steps as in [Section 8.8.7, "Validating Access to Domains."](#) This is to check that you can access the Administration Server when it is running on `IDMHOST2`.

If you are using a split domain topology, perform the same steps to check that you can Access the Administration Server when it is running on `OIMHOST2`.

8.9.4 Failing the Administration Server Back to IDMHOST1

This step checks that you can fail back the Administration Server, that is, stop it on `IDMHOST2` and run it on `IDMHOST1`. To do this, migrate `ADMINVHN` back to `IDMHOST1` node as described in the following steps.

If you are using a split domain topology, follow the same procedures to migrate `OIMADMINVHN` back to `OIMHOST1`.

1. Ensure that the Administration Server is not running. If it is, stop it from the WebLogic console, or by running the command `stopWeblogic.sh` from `ASERVER_HOME/bin`.
2. On `IDMHOST2`, unmount the Administration server domain directory. For example:

```
umount /u01/app/oracle/admin/IDMDomain/aserver/
```
3. On `IDMHOST1`, mount the Administration server domain directory. For example:

```
mount /u01/app/oracle/admin/IDMDomain/aserver/
```
4. Disable the `ADMINVHN.mycompany.com` virtual IP address on `IDMHOST2` and run the following command as `root` on `IDMHOST2`:

```
/sbin/ifconfig x:y down
```

where `x:y` is the current interface used by `ADMINVHN.mycompany.com`.
5. Run the following command on `IDMHOST1`:

```
/sbin/ifconfig interface:index 100.200.140.206 netmask 255.255.255.0
```

Note: Ensure that the netmask and interface to be used match the available network configuration in `IDMHOST1`

6. Update routing tables by using `arping`. Run the following command from `IDMHOST1`.

```
/sbin/arping -b -A -c 3 -I interface 100.200.140.206
```
7. If Node Manager is not already started on `IDMHOST1`, start it, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
8. Start the Administration Server again on `IDMHOST1`.

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

Once in the WLST shell, execute

```
nmConnect(Admin_User, 'Admin_Pasword', IDMHOST1, '5556',
          'IDMDomain', '/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain'
nmStart('AdminServer')
```
9. Test that you can access the Oracle WebLogic Server Administration Console at:
`http://ADMINVHN.mycompany.com:7001/console`
10. Check that you can access and verify the status of components in the Oracle Enterprise Manager at:
`http://ADMINVHN.mycompany.com:7001/em`

8.10 Backing Up the WebLogic Domain

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later

steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information about database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation at this point, complete these steps:

1. Back up the web tier as described in [Section 7.6, "Backing up the Web Tier Configuration."](#)
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.
3. Stop Node Manager and all the processes running in the domain, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
4. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the `ORACLE_BASE/admin/domainName/aserver` directory. On Linux, type:

```
tar -cvf edgdomainback.tar ORACLE_BASE/admin/domain_name/aserver
```

For information about backing up the application tier configuration, see [Section 20.6, "Performing Backups and Recoveries."](#)

Extending the Domain to Include Oracle Internet Directory

This chapter describes how to extend the domain with Oracle Internet Directory (OID) in the enterprise deployment.

This chapter includes the following topics:

- [Section 9.1, "Overview of Extending the Domain to Include Oracle Internet Directory"](#)
- [Section 9.2, "Using Oracle Internet Directory in an Enterprise Deployment"](#)
- [Section 9.3, "Prerequisites for Configuring Oracle Identity Directory Instances"](#)
- [Section 9.4, "Configuring the Oracle Internet Directory Instances"](#)
- [Section 9.5, "Post-Configuration Steps"](#)
- [Section 9.6, "Validating the Oracle Internet Directory Instances"](#)
- [Section 9.7, "Tuning Oracle Internet Directory"](#)
- [Section 9.8, "Backing up the Oracle Internet Directory Configuration"](#)

9.1 Overview of Extending the Domain to Include Oracle Internet Directory

In this chapter, you perform the following tasks:

- Configure two instances of Oracle Internet Directory by using the Oracle Identity Management 11g Configuration Wizard
- Register the instances with the WebLogic Server Domain (IDMDomain).
- Validate the instances
- Tune Oracle Internet Directory

9.2 Using Oracle Internet Directory in an Enterprise Deployment

You use the Identity Store for storing information about users and groups. You use Policy Store for storing information about security policies and for configuration information. Although you can use a single Oracle Internet Directory instance for storing both the identity and policy information, it is recommended that you use two directory stores.

If you intend to separate your identity and policy information, you must create two highly available instances of Oracle Internet Directory. These instances can coexist on

the same nodes or can exist on separate nodes. The data, however, must be stored in two separate databases. If policy information must reside in Oracle Internet Directory, you can place identity information into a different directory, such as Active Directory.

The procedure for installing and configuring the two instances of Oracle Internet Directory is the same. You must, however, point `idstore.mycompany.com` at one of the instances and `policystore.mycompany.com` at the other.

9.3 Prerequisites for Configuring Oracle Identity Directory Instances

Before configuring the Oracle Internet Directory instances on LDAPHOST1 and LDAPHOST2, ensure that the following tasks have been performed:

1. Synchronize the time on the individual Oracle Internet Directory nodes using Greenwich Mean Time so that there is a discrepancy of no more than 250 seconds between them.

Note: If OID Monitor detects a time discrepancy of more than 250 seconds between the two nodes, the OID Monitor on the node that is behind stops all servers on its node. To correct this problem, synchronize the time on the node that is behind in time. The OID Monitor automatically detects the change in the system time and starts the Oracle Internet Directory servers on its node.

2. Install and upgrade the software on LDAPHOST1 and LDAPHOST2 as described in [Section 6.3.4, "Installing Oracle Identity Management."](#)
3. If you plan on provisioning the Oracle Internet Directory instances on shared storage, ensure that the appropriate shared storage volumes are mounted on LDAPHOST1 and LDAPHOST2 as described in [Section 4.4.4, "Directory Structure."](#)
4. Ensure that the load balancer is configured.

Note: Disable the load balancer configuration while configuring Oracle Internet Directory to ensure that Oracle Internet Directory accounts are not locked during configuration.

9.4 Configuring the Oracle Internet Directory Instances

Follow these steps to configure the Oracle Internet Directory components, LDAPHOST1 and LDAPHOST2 on the directory tier with Oracle Internet Directory. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

This section contains the following topics:

- [Section 9.4.1, "Configuring the First Oracle Internet Directory Instance"](#)
- [Section 9.4.2, "Configuring an Additional Oracle Internet Directory Instance"](#)

9.4.1 Configuring the First Oracle Internet Directory Instance

1. Ensure that ports 3060 and 3131 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On Linux:

```
netstat -an | grep "3060"
netstat -an | grep "3131"
```

If the ports are in use (that is, if the command returns output identifying either port), you must free the port.

On Linux:

Remove the entries for ports 3060 and 3131 in the `/etc/services` file and restart the services, or restart the computer.

2. Create a file containing the ports used by Oracle Internet Directory. On Disk1 of the installation media, locate the file `stage/Response/staticports.ini`. Copy it to a file called `oid_ports.ini`. Delete all entries in `oid_ports.ini` except for Non-SSL Port for Oracle Internet Directory and SSL Port for Oracle Internet Directory. Change the values of those ports to 3060 and 3131, respectively.

Note: If the port names in the file are slightly different from those listed in this step, use the names in the file.

3. Start the Oracle Identity Management 11g Configuration Wizard by running `IDM_ORACLE_HOME/bin/config.sh` on Linux or `IDM_ORACLE_HOME\bin\config.bat` on Windows.
4. On the Welcome screen, click **Next**.
5. On the Select Domain screen, select **Configure without a Domain**. Click **Next**.
6. On the Specify Installation Location screen, specify the following values:
 - Oracle Instance Location: `/u01/app/oracle/admin/oid1`
 - Oracle Instance Name: `oid1`
 Click **Next**.
7. On the Specify Email for Security Updates screen, specify these values:
 - Email Address: Provide the email address for your My Oracle Support account.
 - Oracle Support Password: Provide the password for your My Oracle Support account.
 - Check the check box next to the **I wish to receive security updates via My Oracle Support** field.
 Click **Next**.
8. On the Configure Components screen, select **Oracle Internet Directory**, deselect all the other components, and then click **Next**.
9. On the Configure Ports screen, you use the `oid_ports.ini` file you created in Step 2 to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `oid_ports.ini`.

- c. Click **Save**, then click **Next**.
10. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
- **Connect String:**
OIDDBHOST1-vip.mycompany.com:1521:ldmdb1^OIDDBHOST2-vip.mycompany.com:1521:ldmdb2@oidedg.mycompany.com

Notes:

- The Oracle RAC database connect string information must be provided in the format:
host1:port1:instance1^host2:port2:instance2@service_name
 - During this installation, it is not required for all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed. It is required that the information provided is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each Oracle RAC instance, and the service name provided must be configured for all the specified Oracle RAC instances. Any incorrect information entered in the Oracle RAC database connect string has to be corrected manually after the installation.
 - If you are using Oracle Database 11.2, replace the vip addresses and port with the 11.2 SCAN address and port.
-

- **User Name:** ODS
 - **Password:** ***** (enter the password)
- Click **Next**.
11. On the Configure OID screen, specify the following information:
- **Realm:** The realm where you want your company information stored, for example: dc=mycompany, dc=com
 - **Administrator Password:** Password for cn=orcladmin
- Click **Next**.
12. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
13. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.
14. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
15. To validate the installation of the Oracle Internet Directory instance on LDAPHOST1, issue these commands:

```
ldapbind -h LDAPHOST1.mycompany.com -p 3060 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST1.mycompany.com -p 3131 -D "cn=orcladmin" -q -U 1
```

Note: Ensure that the following environment variables are set before using `ldapbind`:

- `ORACLE_HOME` (set to `IDM_ORACLE_HOME`)
 - `ORACLE_INSTANCE`
 - `PATH` - The following directory locations should be in your `PATH`:
 - `ORACLE_HOME/bin`
 - `ORACLE_HOME/ldap/bin`
 - `ORACLE_HOME/ldap/admin`
-

It is recommended that you tune Oracle Internet Directory at this point. See the Oracle Internet Directory chapter in the *Oracle Fusion Middleware Performance and Tuning Guide*.

9.4.2 Configuring an Additional Oracle Internet Directory Instance

The schema database must be running before you perform this task. Follow these steps to install Oracle Internet Directory on LDAPHOST2:

1. Ensure that ports 3060 and 3131 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On Linux:

```
netstat -an | grep "3060"
netstat -an | grep "3131"
```

If the ports are in use (that is, if the command returns output identifying either port), you must free them.

On Linux:

Remove the entries for ports 3060 and 3131 in the `/etc/services` file and restart the services, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

2. Start the Oracle Identity Management 11g Configuration Wizard by running `IDM_ORACLE_HOME/bin/config.sh`.
3. On the Welcome screen, click **Next**.
4. On the Select Domain screen, select **Configure without a Domain**.
Click **Next**.
5. On the Specify Installation Location screen, specify the following values:
Oracle Instance Location: `/u01/app/oracle/admin/oid2`
Oracle Instance Name: `oid2`
Click **Next**.
6. On the Specify Email for Security Updates screen, specify these values:
 - Email Address: Provide the email address for your My Oracle Support account.

- Oracle Support Password: Provide the password for your My Oracle Support account.
- Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

7. On the Configure Components screen, select Oracle Internet Directory, deselect all the other components, and click **Next**.
8. On the Configure Ports screen, you use the `oid_ports.ini` file you created in [Section 9.4.1, "Configuring the First Oracle Internet Directory Instance"](#) to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `oid_ports.ini`.
 - c. Click **Save**, then click **Next**.
9. On the Specify Schema Database screen, select **Use Existing Schema** and specify the following values:
 - Connect String:
`OIDDDBHOST1-vip.mycompany.com:1521:ldmdb1^OIDDDBHOST2-vip.mycompany.com:1521:ldmdb2@oidedg.mycompany.com`

Notes:

- The Oracle RAC database connect string information must be provided in the format:

`host1:port1:instance1^host2:port2:instance2@service_name`
- During this installation, it is not required that all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed.
- You must provide complete and accurate information. Specifically, you must provide the correct host, port, and instance name for each Oracle RAC instance, and the service name you provide must be configured for all the specified Oracle RAC instances.

Any incorrect information entered in the Oracle RAC database connect string must be corrected manually after the installation.

- User Name: ODS
- Password: `*****` (enter the password)

Click **Next**.

10. The ODS Schema in use message appears. The ODS schema chosen is already being used by the existing Oracle Internet Directory instance. Therefore, the new Oracle Internet Directory instance being configured would reuse the same schema.

Choose **Yes** to continue.

A popup window with this message appears:

"Please ensure that the system time on this Identity Management Node is in sync with the time on other Identity management Nodes that are part of the Oracle Application Server Cluster (Identity Management) configuration. Failure to ensure this may result in unwanted instance failovers, inconsistent operational attributes in directory entries and potential inconsistent behavior of password state policies."

Ensure that the system time between IDMHOST1 and IDMHOST2 is synchronized.

Click **OK** to continue.

11. On the Specify OID Admin Password screen, specify the Oracle Internet Directory administration password.

Note: If you see a message saying that OID is not running, verify that the orcladmin account has not become locked and try again. Do not continue until this message is no longer displayed.

Click **Next**.

12. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
13. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.
14. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
15. To validate the installation of the Oracle Internet Directory instance on LDAPHOST2, issue these commands:

```
ldapbind -h LDAPHOST2.mycompany.com -p 3060 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST2.mycompany.com -p 3131-D "cn=orcladmin" -q -U 1
```

Note: Ensure that the following environment variables are set before using ldapbind:

- *ORACLE_HOME*
 - *ORACLE_INSTANCE*
 - *PATH* - The following directory locations should be in your *PATH*:
ORACLE_HOME/bin
ORACLE_HOME/ldap/bin
ORACLE_HOME/ldap/admin
-

9.5 Post-Configuration Steps

Follow the steps in this section to complete the configuration of the Oracle Internet Directory instances.

This section contains the following topics:

- [Section 9.5.1, "Registering Oracle Internet Directory with the WebLogic Server Domain \(IDMDomain\)"](#)
- [Section 9.5.2, "Generating a Certificate to be Used by the Identity Management Domain"](#)
- [Section 9.5.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections"](#)
- [Section 9.5.4, "Validating SSL Manually"](#)
- [Section 9.5.5, "Considering Oracle Internet Directory Password Policies"](#)

9.5.1 Registering Oracle Internet Directory with the WebLogic Server Domain (IDMDomain)

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage the Oracle Internet Directory component with this tool, you must register the component and the Oracle Fusion Middleware instance that contains it with an Oracle WebLogic Server domain. A component can be registered either at install time or post-install. A previously un-registered component can be registered with a WebLogic domain by using the `opmnctl registerinstance` command.

To register the Oracle Internet Directory instances installed on LDAPHOST1 and LDAPHOST2, follow these steps for each instance:

1. Set the `ORACLE_HOME` variable. For example, on LDAPHOST1 and LDAPHOST2, issue this command:

```
export ORACLE_HOME=IDM_ORACLE_HOME
```

2. Set the `ORACLE_INSTANCE` variable. For example:

On LDAPHOST1, issue this command:

```
export ORACLE_INSTANCE=/u01/app/oracle/admin/oid1
```

On LDAPHOST2, issue this command:

```
export ORACLE_INSTANCE=/u01/app/oracle/admin/oid2
```

3. Execute the `opmnctl registerinstance` command on both LDAPHOST1 and LDAPHOST2:

```
ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost WLSHostName -adminPort  
WLSPort -adminUsername adminUserName
```

For example, on LDAPHOST1 and LDAPHOST2:

```
ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost ADMINVHN.mycompany.com  
-adminPort 7001 -adminUsername weblogic
```

The command requires login to WebLogic Administration Server (ADMINVHN.mycompany.com)

Username: weblogic

Password: *****

Note: For additional details on registering Oracle Internet Directory components with a WebLogic Server domain, see the "Registering an Oracle Instance or Component with the WebLogic Server" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

4. On both LDAPHOST1 and LDAPHOST2, update the Enterprise Manager Repository URL using the `emctl` utility with the `switchOMS` flag. This will enable the local emagent to communicate with the WebLogic Administration Server using the virtual IP address. The `emctl` utility is located under the `ORACLE_INSTANCE/EMAGENT/EMAGENT/bin` directory.

Syntax:

```
./emctl switchOMS ReposURL
```

For Example:

```
./emctl switchOMS http://ADMINVHN:7001/em/upload
```

Output:

```
./emctl switchOMS http://ADMINVHN.mycompany.com:7001/em/upload
Oracle Enterprise Manager 10g Release 5 Grid Control 10.2.0.5.0.
Copyright (c) 1996, 2009 Oracle Corporation. All rights reserved.
SwitchOMS succeeded.
```

5. Force the agent to reload its configuration by issuing the command:


```
./emctl reload
```
6. Check that the agent is using the correct Upload URL using the command:


```
./emctl status agent
```
7. Validate that the agents on LDAPHOST1 and LDAPHOST2 are configured properly to monitor their respective targets. Follow these steps to complete this task:
 - Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at:


```
http://ADMINVHN.mycompany.com:7001/em
```

 Log in as the `weblogic` user.
 - From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm** -> **Agent-Monitored Targets**.
 - Update the WebLogic monitoring user name and the WebLogic monitoring password.
 - Enter `weblogic` as the WebLogic monitoring user name and the password for the `weblogic` user as the WebLogic monitoring password.
 - Click **OK** to save your changes.

9.5.2 Generating a Certificate to be Used by the Identity Management Domain

Perform this task after you have registered Oracle Internet Directory with Oracle WebLogic Server.

External domains communicate with the Identity Management domain using SSL Server Authentication Only Mode. To enable the Identity Management domain to support this SSL mode, you must generate a certificate and store it in the Policy Store. This adds an extra layer of security, ensuring that only those domains with access to the security certificate can communicate with the domain. The domain level certificate is generated once per domain.

9.5.2.1 Prerequisites

Note: Using the following approach for SSL configuration requires an LDAP server to be available as a central repository and also available as a demoCA. If you are deploying separate instances for Identity Store and Policy Store, you can use the Policy Store Oracle Internet Directory as the store for the SSL repository.

Prior to running this command ensure that:

- Oracle Identity Management is installed on IDMHOST1.
- Oracle Identity and Access Management is installed on IDMHOST1.
- If you are using Windows, you have installed a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See <http://www.cygwin.com>.

Note: When using Cygwin, ensure that you use the "/" character in path names when exporting a variable. For example:

```
export ORACLE_HOME=c:/oracle/idm
```

9.5.2.2 Generating the Certificate

To generate a certificate for the IDMDomain execute the following commands on IDMHOST1.

1. Set the `ORACLE_HOME` and `JAVA_HOME` variables. For example, issue this command:

```
export ORACLE_HOME=IDM_ORACLE_HOME
export PATH=$JAVA_HOME/bin:$PATH
```

2. Generate the certificate using the `SSLGenCA` command which is located in `ORACLE_COMMON_HOME/bin`

For example:

```
cd ORACLE_COMMON_HOME/bin
./SSLGenCA.sh
```

3. When the command executes supply the following information:

- LDAP host Name: `policystore.mycompany.com`.

Note: It is recommended that you use the Policy Store directory, not the Identity Store.

- LDAP Port: 389
- Admin User: cn=orcladmin
- password: *admin_password*
- LDAP sslDomain where your CA will be stored: IDMDomain
- Password to protect your CA wallet: *wallet_password*
- Confirmed password for your CA wallet: *wallet_password*

Sample output:

SSL Certificate Authority Generation Script: Release 11.1.1.4.0 - Production
Copyright (c) 2010 Oracle. All rights reserved.

```
*****
***** This tool will generate a self-signed CA wallet *****
***** and store it in a central LDAP directory *****
***** for IDM and FA SSL set up and provisioning *****
*****
>>>Enter the LDAP hostname [slc00xx.mycompany.com]: polycystore.mycompany.com
>>>Enter the LDAP port [389]: 389
>>>Enter the admin user [cn=orcladmin]
>>>Enter password for cn=orcladmin:
>>>Enter the LDAP sslDomain where your CA will be stored [idm]: IDMDomain
>>>Enter a password to protect your CA wallet:
>>>Enter confirmed password for your CA wallet:
```

Generate a new CA Wallet...

Create SSL Domains Container for cn=IDMDomain,cn=sslDomains...

Storing the newly generated CA to the LDAP...

Set up ACL to protect the CA wallet...

>>>The newly generated CA is stored in LDAP entry
cn=demoCA,cn=IDMDomain,cn=sslDomains successfully.

This script performs the following tasks:

- Creates a Demo Signing CA wallet for use in the domain.
- Extracts the public Demo CA Certificate from the CA wallet.
- Uploads the wallet and the certificate to LDAP and stores them in the entry:
cn=demoCA,Deployment_SSL_Domain
- Creates an access group in LDAP:
cn=SSLDomains,cn=IDMDomain,cn=demoCA and grants that group administrative privileges to the parent container. All other entities are denied access. Add users to the group to give access. The Demo CA Certificate is now available for download by an anonymous or authenticated user.
- The Demo CA Wallet password is stored locally in an obfuscated wallet for future use. Its path is: *ORACLE_HOME/credCA/castore*

As administrator, you must secure this wallet so that only SSL administrators can read it.

The best place to locate the Certificate is in the Policy Store.

9.5.3 Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections

If you plan to enable SSL Server Authentication Only Mode for your domain and have created a domain level SSL certificate as described in [Section 9.5.2, "Generating a Certificate to be Used by the Identity Management Domain."](#) you must perform the following to ensure that your Oracle Internet Directory instances are capable of accepting requests using this mode. You must configure each Oracle Internet Directory instance independently.

9.5.3.1 Prerequisites

Prior to running this command ensure that:

- Oracle Internet Directory is installed.
- Oracle Identity Management is installed on IDMHOST1
- Site certificate has been generated as described in [Section 9.5.2, "Generating a Certificate to be Used by the Identity Management Domain."](#)
- If you are using Windows, you have installed a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See <http://www.cygwin.com>.

9.5.3.2 Configuring Oracle Internet Directory for SSL

To enable Oracle Internet Directory to communicate using SSL Server Authentication Mode, perform the following steps on LDAPHOST1 and LDAPHOST2:

Note: When you perform this operation, only the Oracle Internet Directory instance you are working on should be running.

1. Set the `ORACLE_HOME`, `ORACLE_INSTANCE` and `JAVA_HOME` variables. For example, on LDAPHOST1, issue this command

```
export ORACLE_HOME=IDM_ORACLE_HOME
export ORACLE_INSTANCE=/u01/app/oracle/admin/oid1
export JAVA_HOME=MW_HOME/jrockit_version
export PATH=$JAVA_HOME/bin:$PATH
```

2. To enable SSL Server Authentication use the tool `SSLServerConfig` which is located in:

```
ORACLE_COMMON_HOME/bin
```

For example

```
$ORACLE_COMMON_HOME/bin/SSLServerConfig.sh -component oid
```

3. When prompted, enter the following information:

- LDAP Hostname: Central LDAP host, for example:
`polycystore.mycompany.com`
- LDAP port: LDAP port, for example: 389
- Admin user DN: `cn=orcladmin`
- Password: `administrator_password`

- sslDomain for the CA: IDMDomain Oracle recommends that the SSLDomain name be the same as the Weblogic domain name to make reference easier.
- Password to protect your SSL wallet/keystore: *password_for_local_keystore*
- Enter confirmed password for your SSL wallet/keystore: *password_for_local_keystore*
- Password for the CA wallet: *certificate_password*. This is the one created in [Section 9.5.2, "Generating a Certificate to be Used by the Identity Management Domain."](#)
- Country Name 2 letter code: Two letter country code, such as US
- State or Province Name: State or province, for example: California
- Locality Name: Enter the name of your city, for example: RedwoodCity
- Organization Name: Company name, for example: mycompany
- Organizational Unit Name: Leave at the default
- Common Name: Name of this host, for example: LDAPHOST1.mycompany.com
- OID component name: Name of your Oracle Instance, for example: oid1. If you need to determine what your OID component name is, execute the command:

ORACLE_INSTANCE/bin/opmnctl status
- WebLogic admin host: Host running the WebLogic Administration Server, for example: adminvhn.mycompany.com
- WebLogic admin port: WebLogic Administration Server port, for example: 7001
- WebLogic admin user: Name of your WebLogic administration user, for example: weblogic
- WebLogic password: *password*.
- AS instance name: Name of the Oracle instance you entered in [Section 9.4.1, "Configuring the First Oracle Internet Directory Instance"](#) and [Section 9.4.2, "Configuring an Additional Oracle Internet Directory Instance,"](#) Step 7, for example: oid1.
- SSL wallet name for OID component [oid_wallet1]: Accept the default
- Do you want to restart your OID component: Yes
- Do you want to test your SSL setup? Yes
- SSL Port of your OID Server: 3131

Sample output:

```
Server SSL Automation Script: Release 11.1.1.4.0 - Production
Copyright (c) 2010 Oracle. All rights reserved.
```

```
Downloading the CA wallet from the central LDAP location...
>>>Enter the LDAP Hostname [slc00dra.mycompany.com]: polycystore.mycompany.com
>>>Enter the LDAP port [3060]: 3060
>>>Enter an admin user DN [cn=orcladmin]
>>>Enter password for cn=orcladmin:
>>>Enter the sslDomain for the CA [idm]: IDMDomain
```

```
>>>Enter a password to protect your SSL wallet/keystore:
>>>Enter confirmed password for your SSL wallet/keystore:
>>>Enter password for the CA wallet:
>>>Searching the LDAP for the CA usercertificate ...
Importing the CA certificate into trust stores...
>>>Searching the LDAP for the CA userpkcs12 ...

Invoking OID SSL Server Configuration Script...
Enter attribute values for your certificate DN
>>>Country Name 2 letter code [US]:
>>>State or Province Name [California]:
>>>Locality Name(eg, city) []:Redwood
>>>Organization Name (eg, company) [mycompany]:
>>>Organizational Unit Name (eg, section) [oid-20110524015634]:
>>>Common Name (eg, hostName.domainName.com) [slc00xxx.mycompany.com]:
The subject DN is
cn=slc00dra.mycompany.com,ou=oid-20110524015634,l=Redwood,st=California,c=US

Creating an Oracle SSL Wallet for oid instance...
/u01/app/oracle/product/fmw/IDM/./oracle_common/bin
>>>Enter your OID component name: [oid1]
>>>Enter the weblogic admin server host [slc00xxx.mycompany.com] ADMINVHN
>>>Enter the weblogic admin port: [7001]
>>>Enter the weblogic admin user: [weblogic]
>>>Enter weblogic password:
>>>Enter your AS instance name:[asinst_1] oid1
>>>Enter an SSL wallet name for OID component [oid_wallet1]
Checking the existence of oid_wallet1 in the OID server...
Configuring the newly generated Oracle Wallet with your OID component...
Do you want to restart your OID component?[y/n]y

Do you want to test your SSL set up?[y/n]y
>>>Please enter your OID ssl port:[3131] 3131
Please enter the OID hostname:[slc00dra.mycompany.com] LDAPHOST1.mycompany.com
>>>Invoking /u01/app/oracle/product/fmw/IDM/bin/ldapbind -h
LDAPHOST1.mycompany.com -p 3131-U 2 -D cn=orcladmin ...
Bind successful

Your oid1 SSL server has been set up successfully
```

Confirm that the script has been successful.

Repeat all the steps in this section, [Section 9.5.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections."](#) for each Oracle Internet Directory instance.

9.5.4 Validating SSL Manually

You can manually verify that the SSL connection has been set up correctly by generating a wallet and then using that wallet to access Oracle Internet Directory. Proceed as follows:

Execute the command

```
./SSLClientConfig.sh -component cacert
```

providing the following inputs:

- LDAP host name: Name of the Oracle Internet Directory server containing the Domain Certificate

- LDAP port: Port used to access Oracle Internet Directory, for example: 3060
- LDAP User: Oracle Internet Directory admin user, for example: cn=orcladmin
- Password: Oracle Internet Directory admin user password
- SSL Domain for CA: This is the value you entered in [Section 9.5.2.2, "Generating the Certificate,"](#) for example, IDMDomain.
- Password for truststore: This is the password you want to assign to your wallet.

When the command executes, it generates wallets in the directory `IDM_ORACLE_HOME/rootCA/keystores/common`

Now that you have a wallet, you can test that authentication is working by executing the command:

```
ldapbind -h LDAPHOST1.mycompany.com -p 3131 -U 2 -D cn=orcladmin -q -W "file:IDM_ORACLE_HOME/rootCA/keystores/common" -Q
```

You will be prompted for your Oracle Internet Directory password and for the wallet password. If the bind is successful, the SSL connection has been set up correctly.

9.5.5 Considering Oracle Internet Directory Password Policies

By default, Oracle Internet Directory passwords expire in 120 days. Users who do not reset their passwords before expiration can no longer authenticate to Oracle Internet Directory. This includes administrative users, such as oamLDAP and oamadmin. Your Identity Management environment cannot work properly unless these users can authenticate. See *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory* for information about changing Oracle Internet Directory password policies.

9.6 Validating the Oracle Internet Directory Instances

To validate the Oracle Internet Directory instances, ensure that you can connect to each Oracle Internet Directory instance and the load balancing router using these commands:

Note: Ensure that the following environment variables are set before using `ldapbind`:

- `ORACLE_HOME` (set to `IDM_ORACLE_HOME`)
 - `ORACLE_INSTANCE`
 - `PATH` - The following directory locations should be in your `PATH`:
`ORACLE_HOME/bin`
`ORACLE_HOME/ldap/bin`
`ORACLE_HOME/ldap/admin`
-

```
ldapbind -h LDAPHOST1.mycompany.com -p 3060 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST1.mycompany.com -p 3131-D "cn=orcladmin" -q -U 1
ldapbind -h LDAPHOST2.mycompany.com -p 3060 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST2.mycompany.com -p 3131-D "cn=orcladmin" -q -U 1
```

```
ldapbind -h idstore.mycompany.com -p 389 -D "cn=orcladmin" -q
ldapbind -h idstore.mycompany.com -p 636 -D "cn=orcladmin" -q -U 1
```

Note: The `-q` option prompts the user for a password. LDAP tools have been modified to disable the options `-w password` and `-P password` when the environment variable `LDAP_PASSWORD_PROMPTONLY` is set to `TRUE` or `1`. Use this feature whenever possible.

9.7 Tuning Oracle Internet Directory

After you deploy Oracle Internet Directory, you must tune it. For general information about tuning Oracle Internet Directory, see the "Oracle Internet Directory Performance Tuning" chapter in *Oracle Fusion Middleware Performance and Tuning Guide*. For details about modifying the values of specific Oracle Internet Directory attributes, see the "Managing Configuration Attributes" chapter in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

In particular, set the following values when deploying Oracle Identity Management for Fusion Applications:

Attribute	Value
<code>orclskiprefinsql</code>	1
<code>orclmaxcc</code>	4
<code>orclserverprocs</code>	4
<code>orclmatchdnenabled</code>	0
<code>orclmaxldapconns</code>	4096

9.8 Backing up the Oracle Internet Directory Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or at a logical point. Create a backup of the installation after verifying that the install so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the Oracle Internet Directory instances in the directory tier:
 - a. Shut down the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:


```
ORACLE_INSTANCE/bin/opmnctl stopall
```
 - b. Create a backup of the Middleware home on the directory tier. On Linux, as the `root` user, type:


```
tar -cvpf BACKUP_LOCATION/dirtier.tar MW_HOME
```
 - c. Create a backup of the Instance home on the directory tier as the `root` user:

```
tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE
```

- d. Start up the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

2. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager.
3. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the `ORACLE_BASE/admin/domainName/aserver` directory. On Linux, type:

```
tar cvf edgdomainback.tar ORACLE_BASE/admin/domainName/aserver
```

Note: Create backups on all machines in the directory tier by following the steps shown in this section.

For more information about backing up the directory tier configuration, see [Section 20.6, "Performing Backups and Recoveries."](#)

Extending the Domain to Include ODSM

This chapter describes how to extend the Identity Management domain to include Oracle Directory Services Manager.

This chapter includes the following topics:

- [Section 10.1, "Overview of Extending the Domain to Include ODSM"](#)
- [Section 10.2, "Prerequisites"](#)
- [Section 10.3, "Extending the Oracle WebLogic Domain IDMDomain"](#)
- [Section 10.4, "Expanding the ODSM Cluster"](#)
- [Section 10.5, "Provisioning the Managed Servers in the Managed Server Directory"](#)
- [Section 10.6, "Configuring ODSM to work with the Oracle Web Tier"](#)
- [Section 10.7, "Validating the Application Tier Configuration"](#)
- [Section 10.8, "Backing Up the Application Tier Configuration"](#)

10.1 Overview of Extending the Domain to Include ODSM

The application tier consists of multiple computers hosting the Oracle Directory Services Manager and Oracle Access Manager instances. In the complete configuration, requests are balanced among the instances on the application tier computers to create a high-performing, fault tolerant application environment.

Oracle Directory Services Manager is a unified graphical user interface (GUI) for managing instances of Oracle Internet Directory and Oracle Virtual Directory. Oracle Directory Services Manager enables you to configure the structure of the directory, define objects in the directory, add and configure users, groups, and other entries.

This chapter describes how to install and configure Oracle Directory Services Manager (ODSM).

10.2 Prerequisites

- Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
- If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 4.4.4, "Directory Structure."](#)

- Ensure that port 7006 is not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On Linux:

```
netstat -an | grep "7006"
```

If the port is in use (if the command returns output identifying the port), you must free it.

On Linux:

Remove the entries for port 7006 in the `/etc/services` file and restart the services, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

10.3 Extending the Oracle WebLogic Domain IDMDomain

Follow these steps to install and configure Oracle Directory Services Manager in the domain IDMDomain:

1. Create a file containing the ports used by ODSM. On Disk1 of the installation media, locate the file `stage/Response/staticports.ini`. Copy it to a file called `odsm_ports.ini`. Delete all entries in `odsm_ports.ini` except for ODSM Server Port No. Change the values of ODSM Server Port No. to 7006.

Note: If the port name in the file is slightly different from those listed in this step, use the name in the file.

2. Start the Oracle Identity Management 11g Configuration Wizard by running the `config.sh` script located under the `IDM_ORACLE_HOME/bin` directory on IDMHOST1. For example:

```
/u01/app/oracle/product/fmw/idm/bin/config.sh
```

3. On the Welcome screen, click **Next**.
4. On the Select Domain screen, select **Extend Existing Domain** and enter the domain details:

- **Hostname:** ADMINVHN.mycompany.com
- **Port:** 7001
- **User Name:** weblogic
- **User Password:** *user password*

Click **Next**.

5. A dialog box with the following message appears:

The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer to the Identity Management documentation for information on how to verify the domain is valid.

Click **Yes** to continue.

This is a benign warning that you can ignore.

6. On the Specify Installation Location screen, specify the following values (the values for the **Oracle Middleware Home Location** and the **Oracle Home Directory** fields are prefilled. The values default to the Middleware home and Oracle home previously installed on IDMHOST1:
 - **Oracle Middleware Home Location:** /u01/app/oracle/product/fmw
 - **Oracle Home Directory:** idm
 - **WebLogic Server Directory:**
/u01/app/oracle/product/fmw/wlserver_10.3
 - **Oracle Instance Location:** /u01/app/oracle/admin/ods_inst1
 - **Oracle Instance Name:** ods_inst1

Click **Next**.
7. On the Specify Email for Security Updates screen, specify these values:
 - **Email Address:** Provide the email address for your My Oracle Support account.
 - **Oracle Support Password:** Provide the password for your My Oracle Support account.
 - Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.
8. On the Configure Components screen, select **Management Components - Oracle Directory Services Manager**.
Deselect all the other components.
Select the **Clustered** check box.
Click **Next**.
9. On the Configure Ports screen, you use the `odsm_ports.ini` file you created in Step 1 to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `odsm_ports.ini`.
 - c. Click **Save**, then click **Next**.
10. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Configure**.
11. On the Configuration Progress screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait until it completes.
12. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

10.4 Expanding the ODSM Cluster

Follow these steps to extend the WebLogic Server domain and install and configure Oracle Directory Service Manager on IDMHOST2:

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST2 as described in [Section 4.4.4, "Directory Structure."](#)
3. Ensure that port number 7006 is not in use by any service on the computer by issuing this command for the operating system you are using. If a port is not in use, no output is returned from the command.

On Linux:

```
netstat -an | grep "7006"
```

If the port is in use (if the command returns output identifying the port), you must free it.

On Linux:

Remove the entries for port 7006 in the `/etc/services` file if the port is in use by a service and restart the services, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

4. Start the Oracle Identity Management 11g Configuration Wizard by running the `config.sh` script located under the `IDM_ORACLE_HOME/bin` directory on IDMHOST2. For example:

```
/u01/app/oracle/product/fmw/idm/bin/config.sh
```

5. On the Welcome screen, click **Next**.
6. On the Select Domain screen, select the **Expand Cluster** option and specify these values:

- **Hostname:** ADMINVHN.mycompany.com
- **Port:** 7001
- **UserName:** weblogic
- **User Password:** *password for the webLogic user*

Click **Next**.

7. A dialog box with the following message appears:

The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer to the Identity Management documentation for information on how to verify the domain is valid.

Click **YES** to continue.

This is a benign warning that you can safely ignore.

8. On the Specify Installation Location screen, specify the following values. The values for the **Oracle Middleware Home Location** and the **Oracle Home Directory** fields are prefilled. The values default to the Middleware home and Oracle home previously installed on IDMHOST1:

- **Oracle Middleware Home Location:** `/u01/app/oracle/product/fmw`

- **Oracle Home Directory:** idm
- **WebLogic Server Directory:**
/u01/app/oracle/product/fmw/wlserver_10.3
- **Oracle Instance Location:** /u01/app/oracle/admin/ods_inst2
- **Oracle Instance Name:** ods_inst2

Click **Next**.

9. On the Email for Security Updates screen, specify these values:

- **Email Address:** Provide the email address for your My Oracle Support account.
- **Oracle Support Password:** Provide the password for your My Oracle Support account.
- Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

10. On the Configure Components screen, de-select all the products and then click **Next**.
11. On the Configure Ports screen, you use the `odsm_ports.ini` file you created in [Section 10.3, "Extending the Oracle WebLogic Domain IDMDomain"](#) to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `odsm_ports.ini`.
 - c. Click **Save**, then click **Next**.
12. On the Installation Summary screen, review the selections to ensure that they are correct (if they are not, click **Back** to modify selections on previous screens), and click **Configure**.
13. On the Configuration Progress screen, multiple configuration assistants are launched in succession; this process can be lengthy. Wait until it completes.
14. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

10.5 Provisioning the Managed Servers in the Managed Server Directory

This section provides the steps to provision the Managed Server on the local disk. Proceed as follows:

1. Stop the ODS instances on both IDMHOST1 and IDMHOST2. Follow the steps in [Section 20.1, "Starting and Stopping Oracle Identity Management Components"](#)
2. On IDMHOST1, pack the Managed Server domain using the `pack` command located under the `ORACLE_COMMON_HOME/common/bin` directory. Make sure to pass `-managed=true` flag to pack the Managed Server. Type:

```
ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true -domain=path_to_
adminServer_domain -template=templateName.jar -template_name=templateName
```

For example

```
ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true
-domain=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar -template_
```

name=ManagedServer_Template

3. Unpack the Managed Server to the managed server directory on IDMHOST1 using the unpack command located under the *ORACLE_COMMON_HOME* /common/bin directory.

```
ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk
-template=templateName.jar -app_dir=path_to_appdir_on_localdisk -overwrite_
domain=true
```

For example:

```
ORACLE_COMMON_HOME/common/bin/unpack.sh
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar -app_
dir=/u01/app/oracle/admin/IDMDomain/mserver/applications -overwrite_domain=true
```

4. Copy the Managed Server template directory from IDMHOST1 to IDMHOST2. For Example:

```
scp -rp /u01/app/oracle/products/fmw/templates
user@IDMHOST2:/u01/app/oracle/products/fmw/templates
```

5. Unpack the Managed Server to the managed server directory on IDMHOST2 using the unpack command located under the *ORACLE_COMMON_HOME* /common/bin directory.

```
ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk
-template=templateName.jar -app_dir=path_to_appdir_on_localdisk
```

For example:

```
ORACLE_COMMON_HOME/common/bin/unpack.sh
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar -app_
dir=/u01/app/oracle/admin/IDMDomain/mserver/applications
```

6. Restart the wls_ods1 and wls_ods2 instances on both IDMHOST1 and IDMHOST2. Follow the steps in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

7. Delete the *ORACLE_BASE*/admin/IDMDomain/aserver/IDMDomain/servers/wls_ods1 directory on IDMHOST1 and the *ORACLE_BASE*/admin/IDMDomain/aserver/IDMDomain/servers/wls_ods2 directory on IDMHOST2.

These directories are created by the Oracle Universal Installer when the domain is originally configured and are no longer required after the provisioning the Managed Server to the managed server directory.

8. Start ODS instances as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

10.6 Configuring ODSM to work with the Oracle Web Tier

This section describes how to configure Oracle Directory Services Manager to work with the Oracle Web Tier.

This section contains the following topics:

- [Section 10.6.1, "Prerequisites"](#)

- [Section 10.6.2, "Configuring Oracle HTTP Servers to Access the ODSM Console"](#)

10.6.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Install Oracle Web Tier on WEBHOST1 and WEBHOST2.
2. Install and configure ODSM on IDMHOST1 and IDMHOST2.
3. Configure the load balancer with a virtual host name (`admin.mycompany.com`) pointing to web servers WEBHOST1 and WEBHOST2.

10.6.2 Configuring Oracle HTTP Servers to Access the ODSM Console

On each of the web servers on WEBHOST1 and WEBHOST2, a file called `admin_vh.conf` was created in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`, as described [Section 8.8.1, "Configuring Oracle HTTP Server for the WebLogic Administration Server."](#) Edit this file and add the following lines within the virtual host definition:

```
<Location /odsm>
    SetHandler weblogic-handler
    WebLogicCluster IDMHOST1.mycompany.com:7006, IDMHOST2.mycompany.com:7006
</Location>
```

Ensure that the new section is within the virtual host definition, like this:

```
NameVirtualHost *:7777

<VirtualHost *:7777>

    ServerName admin.mycompany.com:80
    ServerAdmin you@your.address
    ...

    <Location /odsm>
        SetHandler weblogic-handler
        WebLogicCluster IDMHOST1.mycompany.com:7006, IDMHOST2.mycompany.com:7006
    </Location>

</VirtualHost>
```

Restart the Oracle HTTP Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

10.7 Validating the Application Tier Configuration

Validate the Application Tier configuration as follows:

10.7.1 Validating Browser Connection to ODSM Site

Follow these steps to validate that you can connect the Oracle Directory Services Manager site in a browser:

1. In a web browser, verify that you can connect to Oracle Directory Services Manager (ODSM) at:

```
http://hostname.mycompany.com:port/odsm
```

For example, on IDMHOST1, enter this URL:

`http://IDMHOST1.mycompany.com:7006/odsm`

and on IDMHOST2, enter this URL:

`http://IDMHOST2.mycompany.com:7006/odsm`

2. In a web browser, verify that you can access ODSM through the load balancer address:

`http://admin.mycompany.com/odsm`

10.7.2 Validating ODSM Connections to Oracle Internet Directory

Validate that Oracle Directory Services Manager can create connections to Oracle Internet Directory.

Create a connection to the Oracle Internet Directory on each ODSM instance separately. Even though ODSM is clustered, the connection details are local to each node. Proceed as follows:

1. Launch Oracle Directory Services Manager from IDMHOST1:

`http://IDMHOST1.mycompany.com:7006/odsm`

2. Create a connection to the Oracle Internet Directory virtual host by providing the following information in ODSM:

Server: `oidstore.mycompany.com`

Port: `636`

Enable the SSL option

User: `cn=orcladmin`

Password: `ldap-password`

3. Launch Oracle Directory Services Manager from IDMHOST2.

Follow Step b to create a connection to Oracle Internet Directory from IDMHOST2

`http://IDMHOST2.mycompany.com:7006/odsm`

4. Create a connection to the Oracle Internet Directory virtual host by providing the corresponding information in ODSM

Note: Accept the certificate when prompted.

10.8 Backing Up the Application Tier Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the web tier as described in [Section 7.6, "Backing up the Web Tier Configuration."](#)
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.
3. Back up the application tier instances by following these steps:
 - a. Shut down the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:
`ORACLE_INSTANCE/bin/opmnctl stopall`
 - b. Create a backup of the Middleware home on the application tier. On Linux, as the `root` user, type:
`tar -cvpf BACKUP_LOCATION/apptier.tar ORACLE_BASE`
 - c. Create a backup of the Instance home on the application tier as the `root` user:
`tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE`
 - d. Start up the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:
`ORACLE_INSTANCE/bin/opmnctl startall`
4. Back up the Administration Server domain directory as described in [Section 8.10, "Backing Up the WebLogic Domain."](#)
5. Back up the Oracle Internet Directory as described in [Section 9.8, "Backing up the Oracle Internet Directory Configuration."](#)

For information about backing up the application tier configuration, see [Section 20.6, "Performing Backups and Recoveries."](#)

Preparing Identity and Policy Stores

This chapter describes how to prepare the Identity and Policy Stores in an Oracle Identity Management enterprise deployment.

It contains the following sections:

- [Section 11.1, "Overview of Preparing Identity and Policy Stores"](#)
- [Section 11.2, "Backing up the LDAP Directories"](#)
- [Section 11.3, "Prerequisites"](#)
- [Section 11.4, "Preparing the OPSS Policy Store"](#)
- [Section 11.5, "Preparing the Identity Store"](#)

Before you can use the Policy Store, you must prepare it. This involves creating a JPS Root context, and users and groups required to access the Policy Store, in the Policy Store directory. It also reassociates the domain's internal Policy Store to use the external LDAP Policy Store.

11.1 Overview of Preparing Identity and Policy Stores

To prepare the Policy Store, you create a JPS Root context, and adding users and groups required to access the Policy Store, in the Policy Store directory. You also reassociate the domain's internal Policy Store to use the external LDAP Policy Store.

Preparing the Identity Store involves extending the schema of the directory to support Oracle Access Manager and Oracle Identity Manager, then seeding the Identity Store with system users that will be used when building the Identity Management topology.

11.2 Backing up the LDAP Directories

The procedures described in this chapter change the configuration of the LDAP directories that host the Identity and Policy Stores. Before performing any of these tasks, back up your LDAP directories. See [Section 9.8, "Backing up the Oracle Internet Directory Configuration"](#) and [Section 12.9, "Backing Up the Oracle Virtual Directory Configuration"](#) for more information.

11.3 Prerequisites

Before proceeding, ensure that the following statements are true:

- Oracle Identity Management 11g is installed on IDMHOST1, as described in [Chapter 6, "Installing the Software for an Enterprise Deployment."](#)

- Oracle Internet Directory is installed and configured (if required) as described in [Chapter 9, "Extending the Domain to Include Oracle Internet Directory."](#)
- Non-Oracle Internet Directory directories are installed and available (if required).

11.4 Preparing the OPSS Policy Store

This section describes how to prepare the Oracle Platform Security Services Policy Store.

It contains the following topics:

- [Section 11.4.1, "Creating Policy Store Users and the Policy Container"](#)
- [Section 11.4.2, "Reassociating the Policy and Credential Store"](#)
- [Section 11.4.3, "Associate OIMDomain with Policy and Credential Store"](#)

11.4.1 Creating Policy Store Users and the Policy Container

Perform the following tasks on IDMHOST1:

1. Set the environment variables: MW_HOME, JAVA_HOME, IDM_HOME, and ORACLE_HOME.
 Set IDM_HOME to *IDM_ORACLE_HOME*
 Set ORACLE_HOME to *IAM_ORACLE_HOME*
 Set MW_HOME to *MW_HOME*.
 Set JAVA_HOME to *MW_HOME/jrockit-version*.
2. Create a properties file, called `polycystore.props` with the following contents:


```
POLICYSTORE_HOST: polycystore.mycompany.com
POLICYSTORE_PORT: 389
POLICYSTORE_BINDDN: cn=orcladmin
POLICYSTORE_READONLYUSER: PolicyROUser
POLICYSTORE_READWRITEUSER: PolicyRWUser
POLICYSTORE_SEARCHBASE: dc=mycompany,dc=com
POLICYSTORE_CONTAINER: cn=jpsroot
```

Where:

- POLICYSTORE_HOST and POLICYSTORE_PORT are, respectively, the host and port of your Policy Store directory.
- POLICYSTORE_BINDDN Is an administrative user in the Policy Store directory
- POLICYSTORE_READONLYUSER and POLICYSTORE_READWRITEUSER are the names of Users you want to create in the Policy Store with Read Only and Read/Write privileges.
- POLICYSTORE_SEARCHBASE is the location in the directory where Users and Groups are stored.
- POLICYSTORE_CONTAINER is the name of the container used for OPSS policy information.

After creating the group, the tool adds the `readonlyuser` as a member of the `OrclPolicyAndCredentialReadPrivilegeGroup` and `readwriteuser` as a member of `OrclPolicyAndCredentialWritePrivilegeGroup`.

3. Configure the Policy Store using the command `idmConfigTool` which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

```
idmConfigTool.sh -configPolicyStore input_file=configfile
```

The syntax on Windows is:

```
idmConfigTool.bat -configPolicyStore input_file=configfile
```

For example:

```
idmConfigTool.sh -configPolicyStore input_file=policystore.props
```

When the command runs you are prompted to enter the password of the account you are connecting to the Policy Store with. You are also asked to specify the passwords you want to assign to the accounts:

- POLICYSTORE_READONLYUSER
- POLICYSTORE_READWRITEUSER

Sample command output:

```
Enter Policy Store Bind DN password:
*** Creation of PolicyROUser ***
Apr 5, 2011 4:23:49 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_user.ldif
Enter User Password for PolicyROUser:
Confirm User Password for PolicyROUser:
*** Creation of PolicyRWUser ***
Apr 5, 2011 4:23:58 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_user.ldif
Enter User Password for PolicyRWUser:
Confirm User Password for PolicyRWUser:
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_group.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_
container.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_group_read_
member.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
```

```

/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_group_
write_member.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_tuning.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oid_schemaadmin.ldif
Apr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_user_
aci.ldif
The tool has completed its operation. Details have been logged to
/home/oracle/idmtools/automation.log
pr 5, 2011 4:24:07 AM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: with
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/policystore_user_
priv.ldif

```

Note: While running this command, you might see the following error message:

WARNING: Error in adding in-memory OID search filters.
You may safely ignore this error.

4. Check log file for any errors or warnings and correct them. The file with the name `automation.log` is created in the directory from where you run the tool.

See Also: *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

11.4.2 Reassociating the Policy and Credential Store

To reassociate the policy and credential store with Oracle Internet Directory, use the WLST `reassociateSecurityStore` command. Follow these steps:

1. From `IDMHOST1`, start the WLST shell from the `ORACLE_COMMON_HOME/common/bin` directory. For example, on Linux systems, you would type:

```
./wlst.sh
```

On Windows you would type:

```
./wlst.cmd
```

2. Connect to the WebLogic Administration Server using the following `wlst connect` command.

```
connect("AdminUser", "AdminUserPassword", "t3://hostname:port")
```

For example:

```
connect("weblogic", "admin_password", "t3://ADMINVHN.mycompany.com:7001")
```

3. Run the `reassociateSecurityStore` command as follows:

Syntax:

```
reassociateSecurityStore(domain="domainName",admin="cn=orcladmin",
password="orclPassword",ldapurl="ldap://LDAPHOST:LDAPPORT",servertype="OID",
jpsroot="cn=jpsRootContainer")
```

Note: The admin value is the DN of the LDAP administrator, that is, the user that has administrative level privileges to the Oracle Internet Directory instance that is used as the Policy Store.

For example:

```
reassociateSecurityStore(domain="IDMDomain",admin="cn=orcladmin",
password="password",
ldapurl="ldap://polycystore.mycompany.com:389",servertype="OID",
jpsroot="cn=jpsroot")
```

The output for the command is as follows:

```
Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
For more help, use help(domainRuntime)
```

```
Starting policy store reassociation.
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during
migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Policy store reassociation done.
Starting credential store reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during
migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Audit store reassociation done
Starting audit store reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during
migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Audit store reassociation done
Jps Configuration has been changed. Please restart the application server.
```

4. Restart the WebLogic Administration Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) after the command completes successfully.

11.4.3 Associate OIMDomain with Policy and Credential Store

In [Section 11.4.2, "Reassociating the Policy and Credential Store,"](#) you reassociated the Policy and Credential Store used by IDMDomain with Oracle Internet Directory. In a split domain, you must also associate the second domain with the same policy store. To do this, proceed as follows:

1. From OIMHOST1, start the WLST shell from the *ORACLE_COMMON_HOME/common/bin* directory. For example, on Linux systems, you would type:

```
./wlst.sh
```

On Windows you would type:

```
./wlst.cmd
```

2. Connect to the WebLogic Administration Server using the following WLST connect command:

```
connect("AdminUser", "AdminUserPassword", "t3://hostname:port")
```

For example:

```
connect("weblogic", "admin_password", "t3://OIMADMINVHN.mycompany.com:7001")
```

3. Run the `reassociateSecurityStore` command, which has the following syntax:

```
reassociateSecurityStore(domain="domainName", admin="LDAPadminDN",
password="orclPassword", ldapurl="ldap://LDAPHOST:LDAPPORT", servertype="OID",
jpsroot="cn=jpsRootContainer", join="true")
```

The admin value is the DN of the LDAP administrator, that is, the user that has administrative level privileges to the Oracle Internet Directory instance that is used as the Policy Store.

For example:

```
reassociateSecurityStore(domain="IDMDomain", admin="cn=orcladmin", password="password",
ldapurl="ldap://policystore.mycompany.com:389", servertype="OID",
jpsroot="cn=jpsroot", join="true")
```

The domain name specified in this invocation of the command must be the same as the domain name used during the first `reassociate` command.

Note: The domain entry must be the same as the entry used when the first domain was associated with the policy store.

4. Restart the WebLogic Administration Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

11.5 Preparing the Identity Store

This section describes how to prepare the Identity Store. It contains the following topics:

- [Section 11.5.1, "Creating the Configuration File"](#)
- [Section 11.5.2, "Preparing a Directory for Oracle Access Manager and Oracle Identity Manager"](#)
- [Section 11.5.3, "Creating Users and Groups"](#)
- [Section 11.5.4, "Creating Access Control Lists in Non-Oracle Internet Directory Directories"](#)

11.5.1 Creating the Configuration File

Create a property file, `idstore.props`, to use when preparing the Identity Store. The file will have the following structure:

Oracle Internet Directory Example

```
# Common
IDSTORE_HOST: LDAPHOST1.mycompany.com
IDSTORE_PORT: 3060
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users, dc=mycompany,dc=com
POLICYSTORE_SHARES_IDSTORE: true
# OAM
IDSTORE_OAMADMINUSER: oamadmin
IDSTORE_OAMSOFTWAREUSER: oamLDAP
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
# OAM and OIM
IDSTORE_SYSTEMIDBASE: cn=systemids,dc=mycompany,dc=com
# OIM
IDSTORE_OIMADMINGROUP: OIMAdministrators
IDSTORE_OIMADMINUSER: oimLDAP
# Required due to bug
IDSTORE_OAMADMINUSER : oaamadmin
# Fusion Applications
IDSTORE_READONLYUSER: IDROUser
IDSTORE_READWRITEUSER: IDRWUser
IDSTORE_SUPERUSER: weblogic_fa
# Weblogic
IDSTORE_WLSADMINUSER : weblogic_idm
```

Where:

- `IDSTORE_BINDDN` is an administrative user in the Identity Store Directory
- `IDSTORE_GROUPSEARCHBASE` is the location in the directory where Groups are Stored.
- `IDSTORE_HOST` and `IDSTORE_PORT` are, respectively, the host and port of your Identity Store directory. Specify the back end directory here, rather than OVD. In the case of OID, specify one of the Oracle Internet Directory instances, for example:
OID: LDAPHOST1 and 3060
- `IDSTORE_LOGINATTRIBUTE` is the LDAP attribute which contains the users Login name.
- `IDSTORE_OAMADMINUSER` is the name of the user you want to create as your Oracle Access Manager Administrator.
- `IDSTORE_OAMSOFTWAREUSER` is a user that gets created in LDAP that is used when Oracle Access Manager is running to connect to the LDAP server.
- `IDSTORE_OIMADMINGROUP` Is the name of the group you want to create to hold your Oracle Identity Manager administrative users.
- `IDSTORE_OIMADMINUSER` is the user that Oracle Identity Manager uses to connect to the Identity store.

- IDSTORE_READONLYUSER is the name of a user you want to create which has Read Only permissions on your Identity Store.
- IDSTORE_READWRITEUSER is the name of a user you want to create which has Read/Write permissions on your Identity Store.
- IDSTORE_SUPERUSER is the name of the administration user you want to use to log in to the WebLogic Administration Console in the Oracle Fusion Applications domain.
- IDSTORE_SEARCHBASE is the location in the directory where Users and Groups are stored.
- IDSTORE_SYSTEMIDBASE is the location of a container in the directory where users can be placed when you do not want them in the main user container. This happens rarely but one example is the Oracle Identity Manager reconciliation user which is also used for the bind DN user in Oracle Virtual Directory adapters.
- IDSTORE_USERSEARCHBASE is the location in the directory where Users are Stored.
- OAM11G_IDSTORE_ROLE_SECURITY_ADMIN is the name of the group which is used to allow access to the OAM console.
- POLICystore_SHARES_IDSTORE is set to true for IDM 11g.
- IDSTORE_OAADMINUSER is required because of a bug in idmConfigTool.

11.5.2 Preparing a Directory for Oracle Access Manager and Oracle Identity Manager

This section explains how to deploy Identity Management components to support Active Directory and Oracle Identity Manager as the identity store.

It contains the following topics:

- [Section 11.5.2.1, "Configuring Oracle Internet Directory for Use with Oracle Access Manager and Oracle Identity Manager"](#)
- [Section 11.5.2.2, "Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Manager"](#)

11.5.2.1 Configuring Oracle Internet Directory for Use with Oracle Access Manager and Oracle Identity Manager

Pre-configuring the Identity Store extends the schema in Oracle Internet Directory.

To do this, perform the following tasks on IDMHOST1:

1. Set the environment variables: MW_HOME, JAVA_HOME, IDM_HOME and ORACLE_HOME.
 Set IDM_HOME to *IDM_ORACLE_HOME*
 Set ORACLE_HOME to *IAM_ORACLE_HOME*
2. Configure the Identity Store by using the command `idmConfigTool`, which is located at:
IAM_ORACLE_HOME/idmtools/bin

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

```
idmConfigTool.sh -preConfigIDStore input_file=configfile
```

The syntax on Windows is:

```
idmConfigTool.bat -preConfigIDStore input_file=configfile
```

For example:

```
idmConfigTool.sh -preConfigIDStore input_file=idstore.props
```

When the command runs, you are prompted to enter the password of the account you are connecting to the Identity Store with. This command might take some time to complete.

Sample command output:

```
Enter ID Store Bind DN password:
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idm_
idstore_groups_template.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idm_
idstore_groups_acl_template.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/systemid_pwdpolicy.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/idmtools/templates/oid/idstore_tuning.ldif
May 25, 2011 2:37:18 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING: /u01/app/oracle/product/fmw/iam/idmtools/templates/oid/oid_
schema_extn.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_pwd_
schema_add.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oim_pwd_schema_
add.ldif
May 25, 2011 2:37:19 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_schema_
add.ldif
May 25, 2011 2:37:34 PM oracle.ldap.util.LDIFLoader loadOneLdifFile
INFO: -> LOADING:
/u01/app/oracle/product/fmw/iam/oam/server/oim-intg/schema/OID_oblix_schema_
index_add.ldif
The tool has completed its operation. Details have been logged to
automation.log
```

3. Check the log file for any errors or warnings and correct them. The file with the name **automation.log** is created in the directory from where you run the tool.

Note: You might see a warning messages similar to this in the log.

WARNING: Error indexing displayName

You may safely ignore this error.

Note: In addition to creating users, `idmConfigTool` creates the following groups:

- `orclFAUserReadPrivilegeGroup`
 - `orclFAUserWritePrivilegeGroup`
 - `orclFAUserWritePrefsPrivilegeGroup`
 - `orclFAGroupReadPrivilegeGroup`
 - `orclFAGroupWritePrivilegeGroup`
-
-

See Also: *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

11.5.2.2 Configuring Active Directory for Use with Oracle Access Manager and Oracle Identity Manager

This section describes how to configure Active Directory. Extend the schema in Active Directory as follows.

Note: The order in which you perform the steps is critical!

1. Locate the following files:

```
IDM_ORACLE_
HOME/oam/server/oim-intg/ldif/ad/schema/ADUserSchema.ldif

IDM_ORACLE_HOME/oam/server/oim-intg/ldif/ad/schema/AD_oam_
pwd_schema_add.ldif
```

2. In both these files, replace the `domain-dn` with the appropriate `domain-dn` value
3. Use `ldapadd` from the command line to load the two LDIF files, as follows.

```
ldapadd -h activedirectoryhostname -p activedirectoryportnumber -D AD_
administrator -q -c -f file
```

where `AD_administrator` is a user which has schema extension privileges to the directory

For example:

```
ldapadd -h "ACTIVEDIRECTORYHOST.mycompany.com" -p 389 -D adminuser -q -c -f
ADUserSchema.ldif
```

```
ldapadd -h "ACTIVE_DIRECTORYHOST.mycompany.com" -p 389 -D adminuser -q -c -f AD_
oam_pwd_schema_add.ldif
```

Note: After the `-D` you can specify either a DN or `user@domain.com`.

4. Then go to:

```
MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/oimtemplates
```

Run the following command to extend Active Directory schema:

```
sh extendadschema.sh -h AD_host -p AD_port -D 'administrator@mydomain.com' -AD
"dc=mydomain,dc=com" -OAM true
```

The command is `extendadschema.Excluding Users from OIM Reconcillationbat` on Windows.

11.5.3 Creating Users and Groups

Configure the Identity Store by using the command `idmConfigTool`, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory in which the `idmConfigTool` is run. To ensure that the same file is appended to every time you run the tool, always run the `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

```
idmConfigTool.sh -prepareIDStore mode=all input_file=configfile
```

The syntax on Windows is:

```
idmConfigTool.bat -prepareIDStore mode=all input_file=configfile
```

For example:

```
idmConfigTool.sh -prepareIDStore mode=all input_file=idstore.props
```

When the command runs, it prompts you to enter the password of the account you are connecting to and passwords for the accounts that are being created.

Note: The password must conform to the following rules:

- Six characters or more
 - One or more numeric character
 - Two or more alphabetic characters
 - Start with alphabetic character
 - One or more lowercase character
-

Note: This invocation of `idmConfigTool` creates the group `orclFAOAMUserWritePrivilegeGroup`.

11.5.4 Creating Access Control Lists in Non-Oracle Internet Directory Directories

In the preceding sections, you seeded the Identity Store with users and artifacts for the Oracle components. If your Identity Store is hosted in a non-Oracle Internet Directory directory, such as Microsoft Active Directory, you must set up the access control lists (ACLs) to provide appropriate privileges to the entities you created. This section lists the artifacts created and the privileges required for the artifacts.

- Users and groups. ACLs to the users and groups container are provided in Oracle Internet Directory. Set them manually for other directories. The Oracle Identity Manager/Oracle Access Manager integration and Fusion Applications require the following artifacts to be created in the Identity store.
 - Group with read privileges to the users container (`orclFAUserReadPrivilegeGroup`). Configure the local directory ACLs so that this group has privileges to read all the attributes of the users in the Identity Store.
 - Group with read/write privileges to the users container (`orclFAUserWritePrivilegeGroup`)
 - Group with read privileges to the groups container (`orclFAGroupReadPrivilegeGroup`)
 - Group with read privileges to the groups container (`orclFAGroupWritePrivilegeGroup`)
 - Group with write privileges to a partial set of attributes (`orclFAUserWritePrefsPrivilegeGroup`)

In multidirectory deployments where Oracle Internet Directory is used as a shadow directory, these attributes exist only in Oracle Internet Directory, so no ACL configuration is required in Active Directory. The partial set of attributes is:

- * `orclAccessibilityMode`
- * `orclColorContrast`
- * `orclFontSize`
- * `orclNumberFormat`
- * `orclCurrency`
- * `orclDateFormat`

- * orclTimeFormat
 - * orclEmbeddedHelp
 - * orclFALanguage
 - * orclFATerritory
 - * orclTimeZone
 - * orclDisplayNameLanguagePreference
 - * orclImpersonationGrantee
 - * orclImpersonationGranter
- The user specified by the IDSTORE_READONLYUSER parameter. When you run the `preconfigIDstore` command, this user is assigned to the groups `orclFAUserReadPrivilegeGroup`, `orclFAWritePrefsPrivilegeGroup`, and `orclFAGroupReadPrivilegeGroup`. The user also needs compare privileges to the `userpassword` attribute of the user entry.
 - The user specified by the IDSTORE_READWRITEUSER parameter. It is assigned to the groups `orclFAUserWritePrivilegeGroup` and `orclFAGroupWritePrivilegeGroup`.
 - Systemids. The System ID container is created for storing all the system identifiers. If there is another container in which the users are to be created, that is specified as part of the admin.
 - Oracle Access Manager Admin User. This user is added to the OAM Administrator group, which provides permission for the administration of the Oracle Access Manager Console. No LDAP schema level privileges are required, since this is just an application user.
 - Oracle Access Manager Software User. This user is added to the groups where the user gets read privileges to the container. This is also provided with schema admin privileges.
 - Oracle Identity Manager user `oimLDAP` under System ID container. Password policies are set accordingly in the container. The passwords for the users in the System ID container must be set up so that they do not expire.
 - Oracle Identity Manager administration group. The Oracle Identity Manager user is added as its member. The Oracle Identity Manager admin group is given complete read/write privileges to all the user and group entities in the directory.
 - WebLogic Administrator. This is the administrator of the IDM domain for Oracle Virtual Directory
 - WebLogic Administrator Group. The WebLogic administrator is added as a member. This is the administrator group of the IDM domain for Oracle Virtual Directory.
 - Reserve container. Permissions are provided to the Oracle Identity Manager admin group to perform read/write operations.

Extending the Domain to Include Oracle Virtual Directory

This chapter describes how to extend the Identity Management domain to include Oracle Virtual Directory (OVD).

This chapter includes the following topics:

- [Section 12.1, "Overview of Extending the Domain to Include Oracle Virtual Directory"](#)
- [Section 12.2, "Prerequisites for Configuring Oracle Virtual Directory Instances"](#)
- [Section 12.3, "Configuring the Oracle Virtual Directory Instances"](#)
- [Section 12.4, "Post-Configuration Steps"](#)
- [Section 12.5, "Disable Oracle Virtual Directory LDAP Listeners NIO"](#)
- [Section 12.6, "Validating the Oracle Virtual Directory Instances"](#)
- [Section 12.7, "Creating ODSM Connections to Oracle Virtual Directory"](#)
- [Section 12.8, "Creating Adapters in Oracle Virtual Directory"](#)
- [Section 12.9, "Backing Up the Oracle Virtual Directory Configuration"](#)

12.1 Overview of Extending the Domain to Include Oracle Virtual Directory

Use of Oracle Virtual Directory is strongly recommended for all Identity Store deployments. This includes cases where your Identity Store uses multiple directories or a single directory (including Oracle Internet Directory).

Follow the steps in this chapter to configure the Oracle Virtual Directory components, LDAPHOST1 and LDAPHOST2 on the directory tier with Oracle Virtual Directory. The procedures for the installations are very similar, but the selections in the configuration options screen differ.

12.2 Prerequisites for Configuring Oracle Virtual Directory Instances

Before configuring the Oracle Virtual Directory instances on LDAPHOST1 and LDAPHOST2, ensure that the following tasks have been performed:

1. Install and upgrade the software on LDAPHOST1 and LDAPHOST2 as described in [Chapter 6, "Installing the Software for an Enterprise Deployment."](#)

2. If you plan on provisioning the Oracle Virtual Directory instances on shared storage, ensure that the appropriate shared storage volumes are mounted on LDAPHOST1 and LDAPHOST2 as described in [Section 4.4.4, "Directory Structure."](#)
3. Ensure that the load balancer is configured as describe in [Section 3.2, "About Virtual Server Names Used by the Topologies."](#)

12.3 Configuring the Oracle Virtual Directory Instances

This section contains the following topics:

- [Section 12.3.1, "Configuring the First Oracle Virtual Directory Instance"](#)
- [Section 12.3.2, "Configuring an Additional Oracle Virtual Directory"](#)

12.3.1 Configuring the First Oracle Virtual Directory Instance

1. Ensure that ports 6501 and 7501 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On Linux:

```
netstat -an | grep "6501"  
netstat -an | grep "7501"
```

If the ports are in use (that is, if the command returns output identifying either port), you must free the port.

On Linux:

Remove the entries for ports 6501 and 7501 in the `/etc/services` file and restart the services, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

2. Create a file containing the ports used by Oracle Virtual Directory. On Disk1 of the installation media, locate the file `stage/Response/staticports.ini`. Copy it to a file called `ovd_ports.ini`. Delete all entries in `ovd_ports.ini` except for Non-SSL Port for Oracle Virtual Directory and SSL Port for Oracle Virtual Directory. Change the values of those ports to 6501 and 7501, respectively.

Note: If the port names in the file are slightly different from those listed in this step, use the names in the file.

3. Start the Oracle Identity Management 11g Configuration Wizard by running `IDM_ORACLE_HOME/bin/config.sh`.
4. On the Welcome screen, click **Next**.
5. On the Select Domain screen, select **Configure without a Domain**.
Click **Next**.
6. On the Specify Installation Location screen, specify the following values:
 - Oracle Instance Location: `/u01/app/oracle/admin/ovd1`
 - Oracle Instance Name: `ovd1`

Click **Next**.

7. On the Specify Email for Security Updates screen, specify these values:
 - Email Address: Provide the email address for your My Oracle Support account.
 - Oracle Support Password: Provide the password for your My Oracle Support account.
 - Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

8. On the Configure Components screen, select **Oracle Virtual Directory**, deselect all the other components, and then click **Next**.
9. On the Configure Ports screen, you use the `ovd_ports.ini` file you created in Step 2 to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `ovd_ports.ini`.
 - c. Click **Save**, then click **Next**.
10. On the Specify Virtual Directory screen: In the Client Listeners section, enter:

- LDAP v3 Name Space: `dc=mycompany,dc=com`

In the OVD Administrator section, enter:

- Administrator User Name: `cn=orcladmin`
- Password: `administrator_password`
- Confirm Password: `administrator_password`

Select **Configure the Administrative Server in secure mode**.

Click **Next**.

11. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
12. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

Click **Next**.

13. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
14. To validate the installation of the Oracle Virtual Directory instance on LDAPHOST1, issue these commands:

```
ldapbind -h LDAPHOST1.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST1.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

Note: Ensure that the following environment variables are set before using `ldapbind`:

- `ORACLE_HOME` (set to `IDM_ORACLE_HOME`)
 - `ORACLE_INSTANCE`
 - `PATH` - The following directory locations should be in your `PATH`:
`ORACLE_HOME/bin`
`ORACLE_HOME/ldap/bin`
`ORACLE_HOME/ldap/admin`
-

12.3.2 Configuring an Additional Oracle Virtual Directory

The schema database must be running before you perform this task. Follow these steps to install Oracle Virtual Directory on LDAPHOST2:

1. Ensure that ports 6501 and 7501 are not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On Linux:

```
netstat -an | grep "6501"  
netstat -an | grep "7501"
```

If the ports are in use (that is, if the command returns output identifying either port), you must free the port.

On Linux:

Remove the entries for ports 6501 and 7501 in the `/etc/services` file and restart the services, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

2. Start the Oracle Identity Management 11g Configuration Wizard by running `IDM_ORACLE_HOME/bin/config.sh`.
3. On the Welcome screen, click **Next**.
4. On the Select Domain screen, select **Configure without a Domain**.
Click **Next**.
5. On the Specify Installation Location screen, specify the following values:
Oracle Instance Location: `/u01/app/oracle/admin/ovd2`
Oracle Instance Name: `ovd2`
Click **Next**.
6. On the Specify Email for Security Updates screen, specify these values:
 - **Email Address:** Provide the email address for your My Oracle Support account.
 - **Oracle Support Password:** Provide the password for your My Oracle Support account.
 - Check the check box next to the **I wish to receive security updates via My Oracle Support** field.

Click **Next**.

7. On the Configure Components screen, select Oracle Virtual Directory, deselect all the other components, and click **Next**.
8. On the Configure Ports screen, you use the `ovd_ports.ini` file you created in [Section 12.3.1, "Configuring the First Oracle Virtual Directory Instance"](#) to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `ovd_ports.ini`.
 - c. Click **Save**, then click **Next**.

9. On the Specify Virtual Directory screen: In the Client Listeners section, enter:

- LDAP v3 Name Space: `dc=mycompany,dc=com`

In the OVD Administrator section, enter:

- Administrator User Name: `cn=orcladmin`
- Password: `administrator_password`
- Confirm Password: `administrator_password`

Select **Configure the Administrative Server in secure mode**.

Click **Next**.

10. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not, click **Back** to modify selections on previous screens. When they are correct, click **Configure**.
11. On the Configuration screen, multiple configuration assistants are launched in succession. This process can be lengthy. Wait for the configuration process to finish.

Click **Next**.

12. On the Installation Complete screen, click **Finish** to confirm your choice to exit.
13. To validate the installation of the Oracle Virtual Directory instance on LDAPHOST2, issue these commands:

```
ldapbind -h LDAPHOST2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST2.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

Note: Ensure that the following environment variables are set before using `ldapbind`:

- `ORACLE_HOME` (set to `IDM_ORACLE_HOME`)
- `ORACLE_INSTANCE`
- `PATH` - The following directory locations should be in your `PATH`:

`ORACLE_HOME/bin`

`ORACLE_HOME/ldap/bin`

`ORACLE_HOME/ldap/admin`

12.4 Post-Configuration Steps

This section contains the following topics:

- [Section 12.4.1, "Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain \(IDMDomain\)"](#)
- [Section 12.4.2, "Configuring Oracle Virtual Directory to Accept Server Authentication Only Mode SSL Connections"](#)

12.4.1 Registering Oracle Virtual Directory with the Oracle WebLogic Server Domain (IDMDomain)

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage the Oracle Virtual Directory component with this tool, you must register the component and the Oracle Fusion Middleware instance that contains it with an Oracle WebLogic Server domain. A component can be registered either at install time or post-install. A previously un-registered component can be registered with a WebLogic domain by using the `opmnctl registerinstance` command.

To register the Oracle Virtual Directory instances, follow these steps on LDAPHOST1 and LDAPHOST2 for each instance:

1. Set the `ORACLE_HOME` variable. For example, issue this command:

```
export ORACLE_HOME=IDM_ORACLE_HOME
```

2. Set the `ORACLE_INSTANCE` variable. For example, on LDAPHOST1, issue this command:

```
export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd1
```

On LDAPHOST2, issue this command:

```
export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd2
```

3. Execute the `opmnctl registerinstance` command:

```
ORACLE_INSTANCE/bin/opmnctl registerinstance -adminHost WLSHostName -adminPort  
WLSPort -adminUsername adminUserName
```

For example:

```
ORACLE_INSTANCE/bin/opmnctl registerinstance \  
-adminHost ADMINVHN.mycompany.com -adminPort 7001 -adminUsername weblogic
```

The command requires login to WebLogic Administration Server.

Username: `weblogic`

Password: `password`

Note: For additional details on registering Oracle Virtual Directory components with a WebLogic Server domain, see the "Registering an Oracle Instance Using OPMNCTL" section in *Oracle Fusion Middleware Administrator's Guide for Oracle Virtual Directory*.

4. In order to manage Oracle Virtual Directory by using Oracle Enterprise Manager Fusion Middleware Control, you must update the Enterprise Manager Repository URL to point to the virtual IP address associated with the WebLogic Administration Server. Do this using the `emctl` utility with the `switchOMS` flag. This will enable the local emagent to communicate with the WebLogic

Administration Server using the virtual IP address. The `emctl` utility is located under the `ORACLE_INSTANCE/EMAGENT/EMAGENT/bin` directory.

Syntax:

```
./emctl switchOMS ReposURL
```

For Example:

```
./emctl switchOMS http://ADMINVHN:7001/em/upload
```

Output:

```
./emctl switchOMS http://ADMINVHN.mycompany.com:7001/em/upload
Oracle Enterprise Manager 10g Release 5 Grid Control 10.2.0.5.0.
Copyright (c) 1996, 2009 Oracle Corporation. All rights reserved.
SwitchOMS succeeded.
```

5. Force the agent to reload its configuration by issuing the command:


```
./emctl reload
```
6. Check that the agent is using the correct Upload URL using the command:


```
./emctl status agent
```
7. Validate if the agents on LDAPHOST1 and LDAPHOST2 are configured properly to monitor their respective targets. Follow these steps to complete this task:
 - a. Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://adminvhn.mycompany.com:7001/em`. Log in as the `weblogic` user.
 - b. From the Domain Home Page navigate to the Agent-Monitored Targets page using the menu under **Farm -> Agent-Monitored Targets**
 - c. Update the WebLogic monitoring user name and the WebLogic monitoring password.
 - Enter `weblogic` as the WebLogic monitoring user name and the password for the `weblogic` user as the WebLogic monitoring password.
 - Click **OK** to save your changes.

12.4.2 Configuring Oracle Virtual Directory to Accept Server Authentication Only Mode SSL Connections

Configure Oracle Virtual Directory as follows.

12.4.2.1 Prerequisites

Prior to running this command ensure that:

- Oracle Identity Management is installed
- Oracle Identity and Access Management is installed.
- Site certificate has been generated as described in [Section 9.5.2, "Generating a Certificate to be Used by the Identity Management Domain."](#)
- If you are using Windows, you have installed a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See <http://www.cygwin.com>.

12.4.2.2 Configuring Oracle Virtual Directory for SSL

Before configuring Oracle Virtual Directory for SSL, set the `ORACLE_HOME`, `ORACLE_INSTANCE` and `JAVA_HOME` variables. For example, on LDAPHOST1 issue these commands:

```
export ORACLE_HOME=IDM_ORACLE_HOME
export PATH=$JAVA_HOME/bin:$PATH
export ORACLE_INSTANCE=/u01/app/oracle/admin/ovd1
```

Start the SSL Configuration tool by issuing the command `SSLServerConfig` command which is located in the directory `ORACLE_COMMON_HOME/bin` directory.

For example:

```
ORACLE_COMMON_HOME/bin/SSLServerConfig.sh -component ovd
```

When prompted, enter the following information:

- LDAP Hostname: Central LDAP host, for example:
`policystore.mycompany.com`

Note: It is recommended that you use the Policy Store directory, not the Identity Store.

- LDAP port: LDAP port, for example: 389
- Admin user DN: `cn=orcladmin`
- Password: `administrator_password`
- `sslDomain` for the CA: `IDMDomain`
- Password to protect your SSL wallet/keystore: `password_for_local_keystore`
- Enter confirmed password for your SSL wallet/keystore: `password_for_local_keystore`
- Password for the CA wallet: `certificate_password`. This is the one created in [Section 9.5.2, "Generating a Certificate to be Used by the Identity Management Domain."](#)
- Country Name 2 letter code: Two letter country code, such as US
- State or Province Name: State or province, for example: California
- Locality Name: Enter the name of your city, for example: RedwoodCity
- Organization Name: Company name, for example: mycompany
- Organizational Unit Name: Leave at the default
- Common Name: Name of this host, for example: `LDAPHOST1.mycompany.com`
- OVD Instance Name: for example, `ovd1`. If you need to determine what your OVD component name is, execute the command:

```
ORACLE_INSTANCE/bin/opmnctl status
```

- Oracle instance name: Name of your Oracle instance, for example: `ovd1`
- WebLogic admin host: Host running the WebLogic Administration Server, for example: `adminvhn.mycompany.com`

- WebLogic admin port: WebLogic Administration Server port, for example: 7001
- WebLogic admin user: Name of your WebLogic administration user, for example: `weblogic`
- WebLogic password: *password*.
- SSL wallet name for OVD component [`ovdks1.jks`]: Accept the default

When asked if you want to restart your Oracle Virtual Directory component, enter `Yes`.

When asked if you would like to test your OVD SSL connection, enter `Yes`. Ensure that the test is a success.

Repeat for each Oracle Virtual Directory instance in the configuration, running the command on the appropriate LDAPHOST.

12.5 Disable Oracle Virtual Directory LDAP Listeners NIO

Before you can bind to the LDAP ports on Oracle Virtual Directory you must disable NIO. To do this, perform the following steps on each of the Oracle Virtual Directory instances:

1. Stop Oracle Virtual Directory by typing:

```
ORACLE_INSTANCE/bin/opmnctl stopproc ias-component=ovd1
```

2. Edit the file:

```
ORACLE_INSTANCE/config/OVD/component/listeners.os_xml
```

Change the file in two places, as follows:

- Locate the section for LDAP SSL listener, which looks like this:

```
<ldap version="20" id="LDAP SSL Endpoint">
  <port>7501</port>
  <host>0.0.0.0</host>
  .....
  .....
  <ssl enabled="true">
  <protocols>SSLv3,TLSv1,SSLv2Hello</protocols>
  .....
  .....
  <tcpNoDelay>true</tcpNoDelay>
  <readTimeout>180000</readTimeout>
  </socketOptions>
</ldap>
```

Modify this section so that it looks like this:

```
<ldap version="20" id="LDAP SSL Endpoint">
  <port>7501</port>
  <host>0.0.0.0</host>
  .....
  .....
  <ssl enabled="true">
  <protocols>SSLv3,TLSv1,SSLv2Hello</protocols>
  .....
  .....
  <tcpNoDelay>true</tcpNoDelay>
  <readTimeout>180000</readTimeout>
  </socketOptions>
```

```
<useNIO>false</useNIO>
</ldap>
```

- Locate the section for LDAP non-SSL listener, which looks like this:

```
<ldap version="20" id="LDAP Endpoint">
<port>6501</port>
<host>0.0.0.0</host>
.....
.....
<ssl enabled="false">
.....
.....
<tcpNoDelay>true</tcpNoDelay>
<readTimeout>180000</readTimeout>
</socketOptions>
</ldap>
```

Modify this section so that it looks like this:

```
<ldap version="20" id="LDAP Endpoint">
<port>6501</port>
<host>0.0.0.0</host>
.....
.....
<ssl enabled="false">
.....
.....
<tcpNoDelay>true</tcpNoDelay>
<readTimeout>180000</readTimeout>
</socketOptions>
<useNIO>false</useNIO>
</ldap>
```

3. Save the file.
4. Restart Oracle Virtual Directory using the command:

```
ORACLE_INSTANCE/bin/opmnctl startproc ias-component=ovd1
```

5. Repeat for each Oracle Virtual Directory instance.

12.6 Validating the Oracle Virtual Directory Instances

To validate the Oracle Virtual Directory instances, ensure that you can connect to each Oracle Virtual Directory instance and the load balancing router using these `ldapbind` commands.

Follow the steps in [Section 12.4.2.2, "Configuring Oracle Virtual Directory for SSL"](#) before running the `ldapbind` command with the SSL port.

```
ldapbind -h LDAPHOST1.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h LDAPHOST2.mycompany.com -p 6501 -D "cn=orcladmin" -q
ldapbind -h idstore.mycompany.com -p 389 -D "cn=orcladmin" -q
```

```
ldapbind -h LDAPHOST1.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
ldapbind -h LDAPHOST2.mycompany.com -p 7501 -D "cn=orcladmin" -q -U 1
```

12.7 Creating ODSM Connections to Oracle Virtual Directory

Before you can manage Oracle Virtual Directory you must create connections from ODSM to each of your Oracle Virtual Directory instances. To do this, proceed as follows:

1. Access ODSM through the load balancer at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Follow these steps to create connections to Oracle Virtual Directory:

To create connections to Oracle Virtual Directory, follow these steps. Create connections to each Oracle Virtual Directory node separately. Using the Oracle Virtual Directory load balancer virtual host from ODSM is not supported:

- a. Create a direct connection to Oracle Virtual Directory on LDAPHOST1 providing the following information in ODSM:

```
Host: LDAPHOST1.mycompany.com
Port: 8899 (The Oracle Virtual Directory proxy port)
Enable the SSL option
User: cn=orcladmin
Password: password_to_connect_to_OVD
```

- b. Create a direct connection to Oracle Virtual Directory on LDAPHOST2 providing the following information in ODSM:

```
Host: LDAPHOST2.mycompany.com
Port: 8899 (The Oracle Virtual Directory proxy port)
Enable the SSL option
User: cn=orcladmin
Password: password_to_connect_to_OVD
```

12.8 Creating Adapters in Oracle Virtual Directory

Oracle Virtual Directory communicates with other directories through adapters.

The procedure is slightly different, depending on the directory you are connecting to. The following sections show how to create and validate adapters for supported directories:

- [Section 12.8.1, "Ensuring the Change Log Generation is Enabled in Oracle Internet Directory"](#)
- [Section 12.8.2, "Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory"](#)
- [Section 12.8.3, "Validating the Oracle Virtual Directory Adapters"](#)

12.8.1 Ensuring the Change Log Generation is Enabled in Oracle Internet Directory

Before you create a change log adapter in Oracle Virtual Directory, you must ensure that the back end Oracle Internet Directory servers have changelog generation enabled.

To test whether a directory server has changelog generation enabled, type:

```
ldapsearch -h directory_host -p ldap_port -D bind_dn -q -b '' -s base
'objectclass=*' lastchangenumber
```

For example:

```
ldapsearch -h LDAPHOST1 -p 3060 -D "cn=orcladmin" -q -b '' -s base 'objectclass=*'  
lastchangenumber
```

If the command output includes `lastchangenumber` with a value, changelog generation is enabled. If changelog generation is not enabled, enable it as described in the "Enabling and Disabling Changelog Generation by Using the Command Line" section of *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*.

12.8.2 Creating Oracle Virtual Directory Adapters for Oracle Internet Directory and Active Directory

You can use `idmConfigTool` to create the Oracle Virtual Directory User and Changelog adapters for Oracle Internet Directory and Active Directory. Oracle Identity Manager requires adapters. It is highly recommended, though not mandatory, that you use Oracle Virtual Directory to connect to Oracle Internet Directory.

To do this, perform the following tasks on `IDMHOST1`:

1. Set the environment variables `IDM_HOME` and `ORACLE_HOME`.

Set `IDM_HOME` to `IDM_ORACLE_HOME`

Set `ORACLE_HOME` to `IAM_ORACLE_HOME`

2. Create a properties file for the adapter you are configuring called `ovd1.props`. The contents of this file depends on whether you are configuring the Oracle Internet Directory adapter or the Active Directory Adapter.

- **Oracle Internet Directory adapter properties file:**

```
ovd.host:LDAPHOST1.mycompany.com  
ovd.port:8899  
ovd.binddn:cn=orcladmin  
ovd.password:ovdpassword  
ovd.oamenabled:true  
ovd.ssl:true  
ldap1.type:OID  
ldap1.host:oididstore.mycompany.com  
ldap1.port:3060  
ldap1.binddn:cn=oimLDAP,cn=systemids,dc=mycompany,dc=com  
ldap1.password:oidpassword  
ldap1.ssl:false  
ldap1.base:dc=mycompany,dc=com  
ldap1.ovd.base:dc=mycompany,dc=com  
usecase.type: single
```

- **Active Directory adapter properties file:**

```
ovd.host:LDAPHOST1.mycompany.com  
ovd.port:8899  
ovd.binddn:cn=orcladmin  
ovd.password:ovdpassword  
ovd.oamenabled:true  
ovd.ssl:true  
ldap1.type:AD  
ldap1.host:adidstore.mycompany.com  
ldap1.port:636  
ldap1.binddn:cn=adminuser  
ldap1.password:adpassword  
ldap1.ssl:true  
ldap1.base:dc=mycompany,dc=com  
ldap1.ovd.base:dc=mycompany,dc=com
```



```
usecase.type: single
```

The following list describes the parameters used in the properties file.

- `ovd.host` is the host name of a server running Oracle Virtual Directory.
 - `ovd.port` is the https port used to access Oracle Virtual Directory.
 - `ovd.binddn` is the user DN you use to connect to Oracle Virtual Directory.
 - `ovd.password` is the password for the DN you use to connect to Oracle Virtual Directory.
 - `ovd.oamenabled` is always `true` in Fusion Applications deployments.
 - `ovd.ssl` is set to `true`, as you are using an https port.
 - `ldap1.type` is set to `OID` for the Oracle Internet Directory back end directory or set to `AD` for the Active Directory back end directory.
 - `ldap1.host` is the host on which back end directory is located. Use the load balancer name.
 - `ldap1.port` is the port used to communicate with the back end directory.
 - `ldap1.binddn` is the bind DN of the `oimLDAP` user.
 - `ldap1.password` is the password of the `oimLDAP` user.
 - `ldap1.ssl` is set to `true` if you are using the back end's SSL connection, and otherwise set to `false`. This should always be set to `true` when an adapter is being created for AD.
 - `ldap1.base` is the base location in the directory tree.
 - `ldap1.ovd.base` is the mapped location in Oracle Virtual Directory.
 - `usecase.type` is set to `Single` when using a single directory type.
3. Configure the adapter by using the `idmConfigTool` command, which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOVD input_file=configfile [log_file=logfile]
```

The syntax on Windows is:

```
idmConfigTool.bat -configOVD input_file=configfile [log_file=logfile]
```

For example:

```
idmConfigTool.sh -configOVD input_file=ovd1.props
```

The command requires no input. The output looks like this:

The tool has completed its operation. Details have been logged to logfile

Run this command for each Oracle Virtual Directory instance in your topology, with the appropriate value for `ovd.host` in the property file.

12.8.3 Validating the Oracle Virtual Directory Adapters

Perform the following tasks by using ODSM:

1. Access ODSM at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Connect to Oracle Virtual Directory.
3. Go the **Data Browser** tab.
4. Expand **Client View** so that you can see each of your user adapter root DN's listed.
5. Expand the user adapter root DN, if there are objects already in the back end LDAP server, you should see those objects here.
6. ODSM doesn't support changelog query, so you cannot expand the `cn=changelog` subtree.

Perform the following tasks by using the command-line:

- Validate the user adapters by typing:

```
ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q -b <user_search_base> -s sub "objectclass=inetorgperson" dn
```

For example:

```
ldapsearch -h LDAPHOST1.mycompany.com -p 6501 -D "cn=orcladmin" -q -b "cn=Users,dc=mycompany,dc=com" -s sub "objectclass=inetorgperson" dn
```

Supply the password when prompted.

You should see the user entries that already exist in the back end LDAP server.

- Validate changelog adapters by typing:

```
ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q -b "cn=changelog" -s one "changenumber>=0"
```

For example:

```
ldapsearch -h LDAPHOST1 -p 6501 -D "cn=orcladmin" -q -b "cn=changelog" -s one "changenumber>=0"
```

The command returns logs of data, such as creation of all the users. It returns without error if the changelog adapters are valid.

- Validate lastchangenumber query by typing:

```
ldapsearch -h directory_host -p ldap_port -D "cn=orcladmin" -q -b "cn=changelog" -s base 'objectclass=*' lastchangenumber
```

For example:

```
ldapsearch -h LDAPHOST1 -p 6501 -D "cn=orcladmin" -q -b "cn=changelog" -s base 'objectclass=*' lastchangenumber
```

The command returns the latest change number generated in the back end LDAP server.

12.9 Backing Up the Oracle Virtual Directory Configuration

It is an Oracle best practices recommendation to create a backup file after successfully completing the installation and configuration of each tier or a logical point. Create a backup of the installation after verifying that the install so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. This backup can be discarded once the enterprise deployment setup is complete. After the enterprise deployment setup is complete, the regular deployment-specific Backup and Recovery process can be initiated. More details are described in the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the directory tier:
 - a. Shut down the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:


```
ORACLE_INSTANCE/bin/opmnctl stopall
```
 - b. Create a backup of the Middleware home on the directory tier. On Linux, as the root user, type:


```
tar -cvpf BACKUP_LOCATION/dirtier.tar MW_HOME
```
 - c. Create a backup of the Instance home on the directory tier as the root user:


```
tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE
```
 - d. Start up the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:


```
ORACLE_INSTANCE/bin/opmnctl startall
```
2. Perform a full database backup (either a hot or cold backup). Oracle recommends that you use Oracle Recovery Manager.
3. Back up the Administration Server domain directory. This saves your domain configuration. The configuration files all exist under the `ORACLE_BASE/admin/domainName/aserver` directory. On Linux, type:


```
tar cvf edgdomainback.tar ORACLE_BASE/admin/domainName/aserver
```

Note: Create backups on all machines in the directory tier by following the steps shown in this section.

For more information about backing up the directory tier configuration, see [Section 20.6, "Performing Backups and Recoveries."](#)

Configuring Oracle Access Manager 11g

This chapter describes how to configure Oracle Access Manager 11.1.1 in the Oracle Identity Management enterprise deployment.

This chapter includes the following topics:

- [Section 13.1, "Overview of Configuring Oracle Access Manager"](#)
- [Section 13.2, "About Domain URLs"](#)
- [Section 13.3, "Using Different Directory Configurations"](#)
- [Section 13.4, "Prerequisites"](#)
- [Section 13.5, "Starting Oracle Access Manager Managed Servers"](#)
- [Section 13.6, "Configuring Oracle Access Manager to work with the Oracle Web Tier"](#)
- [Section 13.7, "Configuring Oracle Access Manager"](#)
- [Section 13.8, "Adding the oamadmin Account to Access System Administrators"](#)
- [Section 13.9, "Create Oracle Access Manager Policies for WebGate 11g"](#)
- [Section 13.10, "Creating Oracle Access Manager Key Store"](#)
- [Section 13.11, "Updating Oracle Access Manager System Parameters"](#)
- [Section 13.12, "Backing Up the Application Tier Configuration"](#)

13.1 Overview of Configuring Oracle Access Manager

Oracle Access Manager enables your users to seamlessly gain access to web applications and other IT resources across your enterprise. It provides a centralized and automated single sign-on (SSO) solution, which includes an extensible set of authentication methods and the ability to define workflows around them. It also contains an authorization engine, which grants or denies access to particular resources based on properties of the user requesting access as well as based on the environment from which the request is made. Comprehensive policy management, auditing, and integration with other components of your IT infrastructure enrich this core functionality.

Oracle Access Manager consists of several components, including OAM Server, Oracle Access Manager Console, and WebGates. The OAM Server includes all the components necessary to restrict access to enterprise resources. The Oracle Access Manager Console is the administrative console to Oracle Access Manager. WebGates are web server agents that act as the actual enforcement points for Oracle Access Manager. Follow the instructions in this chapter and [Chapter 19, "Configuring Single](#)

[Sign-on for Administration Consoles in an Enterprise Deployment](#)" to install and configure the Oracle Access Manager components necessary for your enterprise deployment.

13.2 About Domain URLs

Before you complete this chapter, the following URL is available:

Table 13–1 OAM URLs Before Web Tier Configuration

Component	URLs
OAM Console	<code>http://OAMADMINVHN.mycompany.com:7001/oamconsole</code>

After you complete this chapter, the following URL will be available:

Table 13–2 OAM URLs After Web Tier Configuration

Component	URLs	User	SSO User
OAM Console	<code>http://oamadmin.mycompany.com/oamconsole</code>	weblogic	oamadmin

13.3 Using Different Directory Configurations

The enterprise deployment described in this guide shows Oracle Access Manager using Oracle Internet Directory as the only LDAP repository. Oracle Access Manager uses a single LDAP for policy and configuration data. It is possible to configure another LDAP as the Identity Store where users, organizations and groups reside. For example, an Oracle Access Manager instance may use Oracle Internet Directory as its policy and configuration store and point to an instance of Microsoft Active Directory for users and groups.

In addition, the Identity Stores can potentially be front-ended by Oracle Virtual Directory to virtualize the data sources.

To learn more about the different types of directory configuration for Oracle Access Manager, consult the 11g Oracle Access Manager documentation at Oracle Technology Network. Customers considering these variations should adjust their directory tier and Oracle Access Manager deployment accordingly.

13.4 Prerequisites

Before you configure Oracle Access Manager, ensure that the following tasks have been performed on IDMHOST1 and IDMHOST2:

1. Install Oracle WebLogic Server, Oracle Identity Management, and Oracle Identity and Access Management as described in [Chapter 6, "Installing the Software for an Enterprise Deployment."](#)
2. Install the Identity Store, as described in [Chapter 9, "Extending the Domain to Include Oracle Internet Directory"](#) or "Configuring an Identity Store with Multiple Directories" in *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite*.
3. Prepare the Identity and Policy Stores as described in [Chapter 11, "Preparing Identity and Policy Stores."](#)

4. Install Oracle Virtual Directory, if required, as described in [Chapter 12, "Extending the Domain to Include Oracle Virtual Directory."](#)

13.5 Starting Oracle Access Manager Managed Servers

Start the managed servers WLS_OAM1 and WLS_OAM2 by following the procedure in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

13.6 Configuring Oracle Access Manager to work with the Oracle Web Tier

This section describes how to configure Oracle Access Manager to work with the Oracle Web Tier.

This section contains the following topics:

- [Section 13.6.1, "Prerequisites"](#)
- [Section 13.6.2, "Configuring Oracle HTTP Servers to Display Login Page"](#)
- [Section 13.6.3, "Configuring Oracle HTTP Servers to Access Oracle Access Manager Console"](#)

13.6.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Configure Oracle Web Tier on WEBHOST1 and WEBHOST2 as described in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment."](#)
2. Configure the load balancer as described in [Section 3.2, "About Virtual Server Names Used by the Topologies."](#)
3. Configure Oracle Access Manager on IDMHOST1 and IDMHOST2 as described in [Section 13.11, "Updating Oracle Access Manager System Parameters"](#) and [Section 13.5, "Starting Oracle Access Manager Managed Servers."](#)

13.6.2 Configuring Oracle HTTP Servers to Display Login Page

On each of the web servers on WEBHOST1 and WEBHOST2 edit the file *ORACLE_INSTANCE/config/OHS/component/moduleconf/sso_vh.conf*.

Add the following lines in the virtual host definition:

```
<Location /oam>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WebLogicCluster IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100
</Location>
```

If the END user uses the FAAuthScheme to protect its Application Domain, that is, the FusionApplication, then also add:

```
<Location /fusion_apps>
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
    WebLogicCluster IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100
</Location>
```

Ensure that the newly added lines are within the virtual host definition, like this:

```
<VirtualHost *:7777>
  ServerName https://sso.mycompany.com:443
  ServerAdmin you@your.address
  ...

  <Location /oam>
    SetHandler weblogic-handler
    WLPProxySSL ON
    WLPProxySSLPassThrough ON
    WebLogicCluster IDMHOST1.mycompany.com:14100,IDMHOST2.mycompany.com:14100
  </Location>

  <Location /fusion_apps>
    SetHandler weblogic-handler
    WLPProxySSL ON
    WLPProxySSLPassThrough ON
    WebLogicCluster IDMHOST1.mycompany.com:14100,IDMHOST2.mycompany.com:14100
  </Location>

</VirtualHost>
```

13.6.3 Configuring Oracle HTTP Servers to Access Oracle Access Manager Console

On each of the web servers on WEBHOST1 and WEBHOST2, a file called `admin_vh.conf` was created in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`. (See [Section 8.8, "Configuring Oracle HTTP Server for the WebLogic Domain."](#)) Edit this file and add the following lines within the virtual host definition:

```
<Location /oamconsole>
  SetHandler weblogic-handler
  WebLogicHost ADMINVHN
  WebLogicPort 7001
</Location>
```

Ensure that the new section is within the virtual host definition, like this:

```
NameVirtualHost *:7777

<VirtualHost *:7777>

  ServerName admin.mycompany.com:80
  ServerAdmin you@your.address
  ...

  <Location /oamconsole>
    SetHandler weblogic-handler
    WebLogicHost ADMINVHN
    WebLogicPort 7001
  </Location>

</VirtualHost>
```

Restart the Oracle HTTP Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

13.7 Configuring Oracle Access Manager

This section contains the following topics:

- [Section 13.7.1, "Setting a Global Passphrase"](#)
- [Section 13.7.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool"](#)
- [Section 13.7.3, "Validating the Configuration"](#)
- [Section 13.7.4, "Updating Newly-Created Agent"](#)
- [Section 13.7.5, "Updating Existing WebGate Agents"](#)
- [Section 13.7.6, "Perform Bug 13824816 Workaround"](#)
- [Section 13.7.7, "Configuring Oracle Access Manager for Multidirectory Support"](#)

13.7.1 Setting a Global Passphrase

By default, Oracle Access Manager is configured to use the Open security model. If you plan to change this mode using `idmConfigTool`, you must set a global passphrase. Although you need not set the global passphrase and the web gate access password to be the same, it is recommended that you do. You do this by performing the following steps.

1. Log in to the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
as the WebLogic administration user.
2. Click the **System Configuration** tab.
3. Click **Access Manager Settings** located in the Access Manager Settings section.
4. Select **Open** from the **Actions** menu. The access manager settings are displayed.
5. If you plan to use Simple security mode for OAM servers, supply a global passphrase.
6. Click **Apply**.

13.7.2 Configuring Oracle Access Manager by Using the IDM Automation Tool

Now that the initial installation is done and the security model set, the following tasks must be performed:

- Oracle Access Manager must be configured to use an external LDAP Directory (`idstore.mycompany.com`).
- Oracle Access Manager WebGate Agent must be created.
- You perform these tasks by using `idmConfigTool`.

Perform the following tasks on `IDMHOST1`:

1. Set the environment variables `MW_HOME`, `JAVA_HOME`, `IDM_HOME` and `ORACLE_HOME`.
Set `IDM_HOME` to `IDM_ORACLE_HOME`.
Set `ORACLE_HOME` to `IAM_ORACLE_HOME`.
2. Create a properties file called `config_oam1.props` with the following contents:
`WLSHOST: adminvhn.mycompany.com`

```
WLSPORT: 7001
WLSADMIN: weblogic
WLSPASSWD: weblogic password
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_DIRECTORYTYPE:OVD
IDSTORE_BINDDN: cn=orcladmin
IDSTORE_USERNAMEATTRIBUTE: cn
IDSTORE_LOGINATTRIBUTE: uid
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_SEARCHBASE: dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
IDSTORE_OAMSOFTWAREUSER: oamLDAP
IDSTORE_OAMADMINUSER: oamadmin
PRIMARY_OAM_SERVERS: IDMHOST1.mycompany.com:5575, IDMHOST2.mycompany.com:5575
WEBGATE_TYPE: ohsWebgate11g
ACCESS_GATE_ID: Webgate_IDM
OAM11G_IDM_DOMAIN_OHS_HOST:sso.mycompany.com
OAM11G_IDM_DOMAIN_OHS_PORT:443
OAM11G_IDM_DOMAIN_OHS_PROTOCOL:https
OAM11G_WG_DENY_ON_NOT_PROTECTED: false
OAM_TRANSFER_MODE: simple
OAM11G_OAM_SERVER_TRANSFER_MODE:simple
OAM11G_IDM_DOMAIN_LOGOUT_URLS:
/console/jsp/common/logout.jsp,/em/targetauth/emaslogout.jsp
OAM11G_OIM_WEBGATE_PASSWD: webgate password
COOKIE_DOMAIN: .mycompany.com
OAM11G_IDSTORE_ROLE_SECURITY_ADMIN: OAMAdministrators
OAM11G_SSO_ONLY_FLAG: true
OAM11G_OIM_INTEGRATION_REQ: true
OAM11G_IMPERSONATION_FLAG:true
OAM11G_SERVER_LBR_HOST:sso.mycompany.com
OAM11G_SERVER_LBR_PORT:443
OAM11G_SERVER_LBR_PROTOCOL:https
COOKIE_EXPIRY_INTERVAL: 120
OAM11G_OIM_OHS_URL:https://sso.mycompany.com:443/
OAM11G_SERVER_LOGIN_ATTRIBUTE: uid
```

Where:

- WLSHOST and WLSPORT are, respectively, the host and port of your administration server, created in [Chapter 8, "Creating Domains for an Enterprise Deployment."](#) This is the virtual name.
- WLSADMIN and WLSPASSWD are, respectively, the WebLogic administrative user and password you use to log in to the WebLogic console.
- IDSTORE_HOST and IDSTORE _PORT are, respectively, the host and port of your Identity Store directory.
- IDSTORE_BINDDN is an administrative user in the Identity Store directory.
- IDSTORE_USERSEARCHBASE is the container under which Oracle Access Manager searches for the users.
- IDSTORE_GROUPSEARCHBASE is the location in the directory where Groups are stored.
- IDSTORE_SEARCHBASE is the location in the directory where Users and Groups are stored.

- IDSTORE_OAMSOFTWAREUSER is the name of the user you created in [Section 11.5, "Preparing the Identity Store"](#) to be used to interact with LDAP.
- IDSTORE_OAMADMINUSER is the name of the user you created in [Section 11.5, "Preparing the Identity Store"](#) to access your OAM Console.
- PRIMARY_OAM_SERVERS is a comma separated list of your OAM Servers and the proxy ports they use.

Note: To determine the proxy ports your OAM Servers use:

1. Log in to the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
 2. Click the **System Configuration** tab.
 3. Expand **Server Instances** under the Common Configuration section
 4. Click an Oracle Access Manager server, such as **WLS_OAM1**, and click **Open**.
 5. Proxy port is the one shown as **Port**.
-

- ACCESS_GATE_ID is the name you want to assign to the WebGate.
- OAM11G_OIM_WEBGATE_PASSWD is the password you will assign to the WebGate after OIM has been configured
- OAM11G_IDM_DOMAIN_OHS_HOST is the name of the load balancer which is in front of the OHS's.
- OAM11G_IDM_DOMAIN_OHS_PORT is the port that the load balancer listens on.
- OAM11G_IDM_DOMAIN_OHS_PROTOCOL is the protocol to use when directing requests at the load balancer.
- OAM11G_OAM_SERVER_TRANSFER_MODE is the security model that the Oracle Access Manager servers function in, as defined in [Section 13.7.1, "Setting a Global Passphrase."](#)
- OAM11G_IMPERSONATION_FLAG is set to True if you are using Oracle Fusion Applications.
- OAM11G_IDM_DOMAIN_LOGOUT_URLS is set to the various logout URLs.
- OAM11G_SSO_ONLY_FLAG configures Oracle Access Manager as authentication only mode or normal mode, which supports authentication and authorization. This is set to true for Fusion Applications.

If OAM11G_SSO_ONLY_FLAG is true, the OAM Server operates in authentication only mode, where all authorizations return true by default without any policy validations. In this mode, the server does not have the overhead of authorization handling. This is recommended for applications which do not depend on authorization policies and need only the authentication feature of the OAM Server.

If the value is false, the server runs in default mode, where each authentication is followed by one or more authorization requests to the OAM Server. WebGate allows the access to the requested resources or not, based on the responses from the OAM Server.

- OAM11G_SERVER_LBR_HOST is the name of the load balancer fronting your site. This and the following two parameters are used to construct your login URL.
 - OAM11G_SERVER_LBR_PORT is the port that the load balancer is listening on.
 - OAM11G_SERVER_LBR_PROTOCOL is the URL prefix to use.
 - COOKIE_DOMAIN is the domain in which the WebGate functions.
 - WEBGATE_TYPE is the type of WebGate agent you want to create. In this release, the value is ohsWebgate11g.
 - OAM11G_IDSTORE_NAME is the name of the Identity Store. If you already have an Identity Store in place which is different from the default created by this tool, set this parameter to the name of that Identity Store.
 - OAM11G_OIM_OHS_URL is the URL that will be used to access OIM when accessing through the load balancer, after OIM is configured.
 - OAM11G_SERVER_LOGIN_ATTRIBUTE: Setting this to uid ensures that when users log in their username is validated against the uid attribute in LDAP.
3. Configure Oracle Access Manager using the command `idmConfigTool` which is located at:

```
IAM_ORACLE_HOME/idmtools/bin
```

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

```
IAM_ORACLE_HOME/idmtools/bin
```

The syntax of the command on Linux is:

```
idmConfigTool.sh -configOAM input_file=configfile
```

The syntax on Windows is:

```
idmConfigTool.bat -configOAM input_file=configfile
```

For example:

```
idmConfigTool.sh -configOAM input_file=config_oam1.props
```

When the command runs you are prompted to enter the password of the account you are connecting to the Identity Store with. You are also asked to specify the passwords you want to assign to these accounts:

- IDSTORE_PWD_OAMSOFTWAREUSER
 - IDSTORE_PWD_OAMADMINUSER
4. Check the log file for any errors or warnings and correct them. A file named `automation.log` is created in the directory where you run the tool.
5. Restart WebLogic Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

Note: After you run `idmConfigTool`, several files are created that you need for subsequent tasks. Keep these in a safe location.

Two WebGate profiles are created: `Webgate_IDM`, which is a 10g profile, and `Webgate_IDM_11g`, which is an 11g profile. `Webgate_IDM` is used for intercomponent communication and `Webgate_IDM_11g` is used by 11g Webgates.

The following files exist in the directory `ASERVER_HOME/domain_name/output/Webgate_IDM_11g`. You need these when you install the WebGate software.

- `cwallet.sso`
- `ObAccessClient.xml`
- `password.xml`

Additionally, you need the files `aaa_cert.pem` and `aaa_key.pem`, which are located in the directory `ASERVER_HOME/domain_name/output/Webgate_IDM`.

13.7.3 Validating the Configuration

To Validate that this has completed correctly.

1. Access the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Log in as the Oracle Access Manager administration user you created in [Section 11.5, "Preparing the Identity Store."](#)
3. Click the **System Configuration** tab
4. Expand **Access Manager Settings - SSO Agents - OAM Agents**.
5. Click the open folder icon, then click **Search**.
6. You should see the WebGate agents `Webgate_IDM` and `Webgate_IDM_11g`, which you created in [Section 13.7.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool."](#)

13.7.4 Updating Newly-Created Agent

After generating the initial configuration, you must edit the configuration and add advanced configuration entries.

1. Select **System Configuration** Tab
2. Select **Access Manager Settings - SSO Agents - OAM Agent** from the directory tree. Double-click or select the open folder icon.
3. On the displayed search page click **Search** to perform an empty search.
4. Click the Agent `Webgate_IDM`.
5. Select **Open** from the Actions menu.
6. Set **Max Connections** to 4 for all of the OAM Servers listed in the primary servers list.
7. Click **Apply**.

8. Repeat Steps 4 through 7 for the WebGate agent Webgate_IDM_11g.
9. Click **Policy Configuration** tab.
10. Double Click **IAMSuiteAgent** under **Host Identifiers**.
11. Click **+** in the **operations** box.
12. Enter the following information:

Table 13–3 Host Name and Port Values

Host Name	Port
admin.mycompany.com	80
oimadmin.mycompany.com	80

13. Click **Apply**.

13.7.5 Updating Existing WebGate Agents

If you have changed the OAM security model using the idmConfigTool you must change the security model used by any existing Webgates to reflect this change.

To do this, perform the following steps:

1. Log in to the Oracle Access Manager Console as the Oracle Access Manager administration user you created in [Section 11.5, "Preparing the Identity Store,"](#) at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings - SSO Agents**.
4. Click **OAM Agents** and select **Open** from the **Actions** menu.
5. In the Search window, click **Search**.
6. Click each Agent that was not created by idmconfigTool in [Section 13.7.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool"](#), for example: **IAMSuiteAgent**.
7. Set the Security value to the new security model.
Click **Apply**.
8. Restart the managed servers WLS_OAM1 and WLS_OAM2 as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

13.7.6 Perform Bug 13824816 Workaround

Perform the following workaround for Bug 13824816:

1. Log in to the WebLogic Administration Server Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. In the left pane of the console, click **Security Realms**.
3. On the Summary of Security Realms page, click **myrealm** under the Realms table.
4. On the Settings page for myrealm, click the **Roles & Policies** tab.
5. On the Realm Roles page, expand the **Global Roles** entry under the Roles table. This brings up the entry for Roles.
6. Click the **Roles** link to go to the Global Roles page.

7. On the Global Roles page, click the **Admin** role to go to the Edit Global Role page:
8. On the Edit Global Roles page, under the Role Conditions table, click **Add Conditions**.
9. On the Choose a Predicate page, select **Group** from the predicates list and click **Next**.
10. On the Edit Arguments Page, specify `OAMAdministrators` in the **Group Argument** field and click **Add**.
11. Click **Finish** to return to the Edit Global Rule page.
The Role Conditions table now shows the `OAMAdministrators` Group as an entry.
12. Click **Save** to finish adding the Admin role to the `OAMAdministrators` Group.

13.7.7 Configuring Oracle Access Manager for Multidirectory Support

Ensure that the data store configured in Oracle Access Manager refers to the search base used in Oracle Virtual Directory, `dc=mycompany, dc=com`.

Follow these steps to update the search base:

1. Log in to the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click **System Configuration**.
3. Expand **Common Configuration**.
4. Expand **Data Sources**.
5. Expand **User Identity Stores**.
6. Double click the store used with Oracle Virtual Directory.
7. Ensure that the **User search base** and **Group search base** fields have the value `dc=mycompany, dc=com`.

13.8 Adding the oamadmin Account to Access System Administrators

The `oamadmin` user is assigned to the Oracle Access Manager Administrators group, which is in turn assigned to the Access System Administrators group. Fusion Applications, however, requires the `oamadmin` user to be explicitly added to that role. To do this perform the following steps:

1. Log in to the oamconsole at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click the **System Configuration** tab.
3. Expand **Data Sources - User Identity Stores**.
4. Click **OIMIDStore**.
5. Click **Open**.
6. Click the **+** symbol next to **Access System Adminsitrators**.
7. Type `oamadmin` in the search box and click **Search**.
8. Click the returned `oamadmin` row, then click **Add Selected**.
9. Click **Apply**.

13.9 Create Oracle Access Manager Policies for WebGate 11g

In order to allow WebGate 11g to display the credential collector, you must add /oam to the list of public policies.

Proceed as follows:

1. Log in to the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Select the **Policy Configuration** tab.
3. Expand **Application Domains - IAM Suite**
4. Click **Resources**.
5. Click **Open**.
6. Click **New resource**.
7. Provide the following values:
 - **Type:** HTTP
 - **Description:** OAM Credential Collector
 - **Host Identifier:** IAMSuiteAgent
 - **Resource URL:** /oam
 - **Protection Level:** Unprotected
 - **Authentication Policy:** Public Policy
8. Click **Apply**.

13.10 Creating Oracle Access Manager Key Store

If you are integrating other components, such as Oracle Identity Manager and Oracle Adaptive Access Manager, with Oracle Access Manager and Oracle Access Manager is using the simple security transport model, you must generate a keystore that can be used with those components. The procedure to do this is outlined in this section. Run it on IDMHOST1.

This section contains the following topics:

- [Section 13.10.1, "Creating an Empty Trust Store File Named oamclient-truststore.jks"](#)
- [Section 13.10.2, "Importing the CA Certificate into the Trust Store"](#)
- [Section 13.10.3, "Setting up Keystore with the SSL Certificate and Private Key File of the Access Client"](#)

13.10.1 Creating an Empty Trust Store File Named oamclient-truststore.jks

To create this file, you use a tool called `keytool` that comes with the JDK (Java Development Kit).

Before running any of the following commands, ensure that the JDK is in your path. For example

```
export JAVA_HOME=MW_HOME/jrockit_version
export PATH=$JAVA_HOME/bin:$PATH
```

1. First, execute the command:


```
keytool -genkey -alias alias_name -keystore PathName_to_Keystore -storetype JKS
```

The command prompts you for a keystore password. This password **MUST** be same as the global pass phrase used in the Oracle Access Manager server. The command also prompts for information about the user and organization. Enter relevant information.

Example:

```
keytool -genkey -alias oam -keystore oamclient-truststore.jks -storetype JKS
```

Sample output:

```
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: John Doe
What is the name of your organizational unit?
[Unknown]: MAA
What is the name of your organization?
[Unknown]: Oracle
What is the name of your City or Locality?
[Unknown]: Redwood Shores
What is the name of your State or Province?
[Unknown]: CA
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=John Doe, OU=MAA, O=Oracle, L=Redwood Shores, ST=CA, C=US correct?
[no]: yes
```

```
Enter key password for <oam>
(RETURN if same as keystore password):
Re-enter new password:
```

2. Then execute the command:

```
keytool -delete -alias alias_name -keystore oamclient-truststore.jks -storetype JKS
```

For example:

```
keytool -delete -alias oam -keystore oamclient-truststore.jks -storetype JKS
```

The command prompts for the keystore password you entered previously.

13.10.2 Importing the CA Certificate into the Trust Store

Oracle Access Manager 11g comes with a self-signed Certificate Authority that is used in Simple mode to issue certificates for the Access Client. This certificate must be added to the keystore you just created.

The certificate resides in the file `cacert.der`, which is located in the directory `IAM_ORACLE_HOME/oam/server/config`. Execute the following command to import a PEM/DER format CA certificate into the trust store. On Linux, type:

```
keytool -importcert -file IAM_ORACLE_HOME/oam/server/config/cacert.der
-trustcacerts -keystore PathName_to_keystore -storetype JKS
```

On Windows, type:

```
keytool -import -file IAM_ORACLE_HOME\oam\server\config\cacert.der -trustcacerts
-keystore PathName_to_keystore -storetype JKS
```

Enter keystore password when prompted.

Example:

```
keytool -importcert -file /IAM_ORACLE_HOME/oam/server/config/cacert.der
-trustcacerts -keystore oamclient-truststore.jks -storetype JKS
```

Sample output:

```
Enter keystore password:
Owner: CN=NetPoint Simple Security CA - Not for General Use, OU=NetPoint,
O="Oblix, Inc.", L=Cupertino, ST=California, C=US
Issuer: CN=NetPoint Simple Security CA - Not for General Use, OU=NetPoint,
O="Oblix, Inc.", L=Cupertino, ST=California, C=US
Serial number: 0
Valid from: Wed Apr 01 05:57:22 PDT 2009 until: Thu Mar 28 05:57:22 PDT 2024
Certificate fingerprints:
MD5: 05:F4:8C:84:85:37:DB:E3:66:87:EF:39:E0:E6:B2:3F
SHA1: 97:B0:F8:19:7D:0E:22:6B:40:2A:73:73:1B:27:B2:7B:8D:64:82:21
Signature algorithm name: MD5withRSA
Version: 1
Trust this certificate? [no]: yes
Certificate was added to keystore
```

13.10.3 Setting up Keystore with the SSL Certificate and Private Key File of the Access Client

An SSL certificate and private key were generated when you ran the `idmConfigTool` command in [Section 13.7.2, "Configuring Oracle Access Manager by Using the IDM Automation Tool."](#) The SSL certificate and key are required for clients to communicate with Oracle Access Manager in Simple mode. The names of these files are, respectively, `aaa_cert.pem` and `aaa_key.pem`. They are located in the directory `ASERVER_HOME/domain_name/output/Webgate_IDM` on `IDMHOST1`, where `ASERVER_HOME` is the Administration Server Domain home.

Execute the following commands to import the certificate and key file into the keystore file `ssoKeystore.jks`.

1. Unzip the file `importcert.zip`, which is located in the directory:

```
IAM_ORACLE_HOME/oam/server/tools/importcert
```

For example:

```
cd IAM_ORACLE_HOME/oam/server/tools/importcert
unzip importcert.zip
```

2. Execute the command:

```
openssl pkcs8 -topk8 -nocrypt -in ASERVER_HOME/domain_name/output/Webgate_
IDM/aaa_key.pem -inform PEM -out aaa_key.der -outform DER
```

The command prompts for a passphrase. Enter the password, which must be the WebGate access password. This command creates the `aaa_key.der` file in the directory where the command is run

Example:

```
openssl pkcs8 -topk8 -nocrypt -in
/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/output/Webgate_IDM/aaa_
key.pem -inform PEM -out aaa_key.der -outform DER
Enter pass phrase for
/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/output/Webgate_IDM/aaa_
key.pem:
```

3. Then execute:

```
openssl x509 -in
/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain/output/Webgate_IDM/aaa_
cert.pem -inform PEM -out aaa_cert.der -outform DER
```

This command creates the `aaa_cert.der` file in the directory where the command is run. This command does not generate any output.

4. Execute the command:

```
java -cp IAM_ORACLE_HOME/oam/server/tools/importcert/importcert.jar
oracle.security.am.common.tools.importcerts.CertificateImport -keystore
ssoKeystore.jks -privatekeyfile aaa_key.der -signedcertfile aaa_cert.der
-storetype jks -genkeystore yes
```

This command creates the `ssoKeystore.jks` file in the directory where the command is run.

In this command, `aaa_key.der` and `aaa_cert.der` are, respectively, the private key and certificate pair in DER format.

Sample output:

```
Enter Keystore password:
Certificates imported to ssoKeystore.jks
```

5. Add the CA certificate to the newly generated ssoKeystore.jks. On Linux, type:

```
keytool -importcert -file IAM_ORACLE_HOME/oam/server/config/cacert.der
-trustcacerts -keystore PathName_to_keystore -storetype JKS
```

On Windows, type:

```
keytool -import -file IAM_ORACLE_HOME\oam\server\config\cacert.der
-trustcacerts -keystore PathName_to_keystore -storetype JKS
```

Enter keystore password when prompted. For example:

```
keytool -importcert -file /IAM_ORACLE_HOME/oam/server/config/cacert.der
-trustcacerts -keystore ssoKeystore.jks -storetype JKS
```

Note: The files `ssoKeystore.jks` and `oamclient-truststore.jks` are required when you integrate Oracle Access Manager running in Simple mode with Oracle Identity Manager. When you integrate these components, you are asked to copy these files to the `ASERVER_HOME/config/fmwconfig` directory. If you subsequently extend the domain on machines where these files have been placed using `pack/unpack`, you must recopy `ssoKeystore.jks` and `oamclient-truststore.jks` after unpacking.

13.11 Updating Oracle Access Manager System Parameters

Update `ASERVER_HOME/config/fmwconfig/oam-config.xml` in the administration server domain home.

Set the parameters `Timeout`, `Expiry`, and `MaxSessionsPerUser` as follows:

1. Log in to the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) as the WebLogic administration user.
2. Select the **System Configuration** tab.
3. Click **Common Settings** under the **Common Configuration** entry.
4. Click **Open**.
5. Set the following values:
 - **Idle Timeout (minutes):** 120
 - **Session Lifetime:** 120
 - **Maximum Number of Sessions per user:** 200
6. Click **Apply**.

13.12 Backing Up the Application Tier Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the web tier as described in [Section 7.6, "Backing up the Web Tier Configuration."](#)
2. Back up the Oracle Access Manager database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.
3. Back up the Administration Server domain directory as described in [Section 8.10, "Backing Up the WebLogic Domain."](#)
4. Back up the Oracle Internet Directory as described in [Section 9.8, "Backing up the Oracle Internet Directory Configuration."](#)
5. Back up the Oracle Virtual Directory as described in [Section 12.9, "Backing Up the Oracle Virtual Directory Configuration."](#)

For information about backing up the application tier configuration, see [Section 20.6, "Performing Backups and Recoveries."](#)

Configuring Oracle Identity Manager

This chapter describes how to configure Oracle Identity Manager for use in the Oracle Identity Management Enterprise Deployment Topology.

This chapter contains the following topics:

- [Section 14.1, "Overview of Configuring Oracle Identity Manager"](#)
- [Section 14.2, "About Domain URLs"](#)
- [Section 14.3, "Prerequisites"](#)
- [Section 14.4, "About the Split Oracle Identity Manager Domain"](#)
- [Section 14.5, "Synchronize System Clocks"](#)
- [Section 14.6, "Configuring Oracle Identity Manager"](#)
- [Section 14.7, "Configuring Oracle Coherence for Deploying Composites"](#)
- [Section 14.8, "Post-Installation Steps on OIMHOST1"](#)
- [Section 14.9, "Post-Installation Steps on OIMHOST2"](#)
- [Section 14.10, "Modifying the Oracle Identity Manager Properties to Support Active Directory"](#)
- [Section 14.11, "Configuring Oracle Identity Manager to Reconcile from ID Store"](#)
- [Section 14.12, "Configuring Oracle Identity Manager to Work with the Oracle Web Tier"](#)
- [Section 14.13, "Configuring a Default Persistence Store for Transaction Recovery"](#)
- [Section 14.14, "Configuring an IT Resource Instance for Email"](#)
- [Section 14.15, "Enabling Oracle Identity Manager to Connect to SOA Using the Administrative Users Provisioned in LDAP"](#)
- [Section 14.16, "Updating the Username Generation Policy for Active Directory"](#)
- [Section 14.17, "Tuning Oracle Platform Security"](#)
- [Section 14.18, "Provisioning Users to the Enterprise Identity Store in a Multidirectory Scenario."](#)
- [Section 14.19, "Excluding Users from Oracle Identity Manager Reconciliation."](#)
- [Section 14.20, "Backing Up the Application Tier Configuration"](#)

14.1 Overview of Configuring Oracle Identity Manager

Oracle Identity Manager is a user provisioning and administration solution that automates the process of adding, updating, and deleting user accounts from applications and directories. It also improves regulatory compliance by providing granular reports that attest to who has access to what. Oracle Identity Manager is available as a standalone product or as part of Oracle Identity Management.

Automating user identity provisioning can reduce Information Technology (IT) administration costs and improve security. Provisioning also plays an important role in regulatory compliance. Key features of Oracle Identity Manager include password management, workflow and policy management, identity reconciliation, reporting and auditing, and extensibility through adapters.

Oracle Identity Manager provides the following key functionalities:

- User Administration
- Workflow and Policy
- Password Management
- Audit and Compliance Management
- Integration Solutions
- User Provisioning
- Organization and Role Management

For details about Oracle Identity Manager, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

14.2 About Domain URLs

After you complete this chapter, the following URL will be available:

Table 14–1 OIM URLs

Topology	Component	URLs	SSO User
All	Self-service Console	https://sso.mycompany.com/oim	xelsysadm

14.3 Prerequisites

Before extending the domain with Oracle Identity Manager, ensure that the following tasks have been performed:

1. Ensure that the virtual IP addresses for the Oracle Identity Manager and SOA managed servers have been provisioned. See [Section 3.5, "About IP Addresses and Virtual IP Addresses"](#) for details
2. Install and upgrade the following software on IDMHOST1, IDMHOST2, OIMHOST1 and OIMHOST2 as described in [Chapter 6, "Installing the Software for an Enterprise Deployment."](#)
 - WebLogic Server
 - Oracle Identity Management
 - Oracle SOA Suite
 - Oracle Identity and Access Management

3. Ensure that you have created the `wlfullclient.jar` file, as described in [Section 6.3.7.3, "Creating the wlfullclient.jar File."](#)
4. Ensure the Identity Store is installed and configured, as described in [Chapter 9](#).
5. Provision the Oracle Identity Management users as described in [Section 11.5, "Preparing the Identity Store."](#)
6. Stop all the managed servers running in your domain, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) before extending the domain with Oracle Identity Manager.

Note: Oracle SOA deployed along with Oracle Identity Manager is used exclusively for Oracle Identity Manager work flow. It cannot be used for other purposes.

14.4 About the Split Oracle Identity Manager Domain

The examples in this chapter show extending the domain `IDMDomain` to include Oracle Identity Manager. If you are building a split domain topology, substitute `OIMDomain` wherever you see a reference to `IDMDomain` and `OIMADMINVHN` wherever you see `ADMINVHN`.

14.5 Synchronize System Clocks

Oracle SOA uses Quartz to maintain its jobs and schedules in the database. Synchronize the system clocks for the SOA WebLogic cluster to enable proper functioning of jobs, adapters, and Oracle B2B.

14.6 Configuring Oracle Identity Manager

You must configure the Oracle Identity Manager server instance before you can start the Oracle Identity Manager and SOA Managed Servers. For a single domain topology this is performed on `IDMHOST1`. For a split domain topology, this is performed on `OIMHOST1`. The Oracle Identity Management Configuration Wizard loads the Oracle Identity Manager metadata into the database and configures the instance.

Before proceeding, ensure that the following are true:

- The Administration Server is up and running.
- The environment variables `DOMAIN_HOME` and `WL_HOME` are *not* set in the current shell.

The Oracle Identity Management Configuration Wizard is located under the Identity Management Oracle home. To start the Configuration Wizard, type:

```
IAM_ORACLE_HOME/bin/config.sh
```

Proceed as follows:

1. On the Welcome screen, click **Next**
2. On the Components to Configure screen, Select **OIM Server**.

Note: Oracle Identity Manager Remote Manager is optional in Fusion Applications implementations

Click **Next**.

3. On the Database screen, provide the following values:

- **Connect String:** The connect string for the Oracle Identity Manager database:
`idmdb1-vip.mycompany.com:1521:oimedg1^idmdb2-vip.mycompany.com:1521:oimedg2@oimedg.mycompany.com`

If you are using Oracle Database 11.2, replace the vip address and port with the 11.2 SCAN address and port.

- **OIM Schema User Name:** `edg_oim`
- **OIM Schema password:** `password`
- **MDS Schema User Name:** `edg_mds`
- **MDS Schema Password:** `password`

Click **Next**.

4. On the WebLogic Administration Server screen, provide the following details for the WebLogic Administration Server:

- **URL:** The URL to connect to the WebLogic Administration Server. For example:

- IDMDomain

`t3://ADMINVHN.mycompany.com:7001`

- OIMDomain

`t3://OIMADMINVHN.mycompany.com:7001`

- **UserName:** `weblogic`
- **Password:** Password for the `weblogic` user

Click **Next**.

5. On the OIM Server screen, provide the following values:

- **OIM Administrator Password:** Password for the Oracle Identity Manager Administrator. This is the password for the `xelsysadm` user. The password must contain an uppercase letter and a number. Best practice is to use the same password that you assigned to the user `xelsysadm` in [Section 11.5, "Preparing the Identity Store."](#)
- **Confirm Password:** Confirm the password.
- **OIM HTTP URL:** Proxy URL for the Oracle Identity Manager Server. This is the URL for the Hardware load balancer that is front ending the OHS servers for Oracle Identity Manager. For example:
`http://idminternal.mycompany.com:80.`
- **Key Store Password:** Key store password. The password must have an uppercase letter and a number.

Click **Next**.

6. On the BI Publisher screen, provide the following values:

- **Configure BI Publisher:** Select if you want to Configure Oracle Identity Manager with Oracle BI Publisher. This is Optional and depends on your requirements.
- **BI Publisher URL:** The URL of BI Publisher, if you selected it.

- **Enable LDAP Sync:** Selected.

Notes: BI Publisher is not a part of the *IDMDomain*. The steps to configure the BI Publisher are not covered in this Enterprise Deployment Guide.

Click **Next**.

7. On the LDAP Server Screen, the information you enter is dependent on your implementation. Provide the following details:
 - **Directory Server Type:**
 - OID, if your Identity Store is in Oracle Internet Directory.
 - OVD if you access your Identity Store through Oracle Virtual Directory.
 - **Directory Server ID:** A name for your Oracle Internet Directory server. For example: IdStore. This is only required if the directory type is OID.
 - **Server URL:** The LDAP server URL. For example:
ldap://idstore.mycompany.com:389
 - **Server User:** The user name for connecting to the LDAP Server. For example:
cn=oimLDAP,cn=systemids,dc=mycompany,dc=com
 - **Server Password:** The password for connecting to the LDAP Server.
 - **Server Search DN:** The Search DN, if you are accessing your IDStore using Oracle Virtual Directory Server. For example: dc=mycompany,dc=com.

Click **Next**.

8. On the LDAP Server Continued screen, provide the following LDAP server details:
 - **LDAP Role Container:** The DN for the Role Container. This is the container where the Oracle Identity Manager roles are stored. For example:
cn=Groups,dc=mycompany,dc=com
 - **LDAP User Container:** The DN for the User Container. This is the container where the Oracle Identity Manager users are stored. For example:
cn=Users,dc=mycompany,dc=com
 - **User Reservation Container:** The DN for the User Reservation Container. For example: cn=Reserve,dc=mycompany,dc=com.

Click **Next**.

9. On the Configuration Summary screen, verify the summary information.
Click **Configure** to configure the Oracle Identity Manager instance
10. On the Configuration Progress screen, once the configuration completes successfully, click **Next**.
11. On the Configuration Complete screen, view the details of the Oracle Identity Manager Instance configured.
Click **Finish** to exit the Configuration Wizard.
12. Restart WebLogic Administration Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.7 Configuring Oracle Coherence for Deploying Composites

Although deploying composites uses multicast communication by default, Oracle recommends using unicast communication in SOA enterprise deployments. Use unicast if you disable multicast communication for security reasons.

Unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster can discover one of the existing nodes. As a result, when a new node has joined the cluster, it is able to discover all of the other nodes in the cluster. Additionally, in configurations such as SOA enterprise deployments where multiple IPs are available in the same system, you must configure Oracle Coherence to use a specific host name to create the Oracle Coherence cluster.

Note: An incorrect configuration of the Oracle Coherence framework used for deployment may prevent the SOA system from starting. The deployment framework must be properly customized for the network environment on which the SOA system runs. Oracle recommends the configuration described in this section.

14.7.1 Enabling Communication for Deployment Using Unicast Communication

Specify the nodes using the `tangosol.coherence.wka<n>` system property, where `<n>` is a number between 1 and 9. You can specify up to 9 nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the virtual host name used by the SOA server as the listener addresses (SOAHOST1VHN and SOAHOST2VHN). Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab.

Tip: To guarantee high availability during deployments of SOA composites, specify enough nodes so that at least one of them is running at any given time.

Note: SOAHOST1VHN is the virtual host name that maps to the virtual IP where WLS_SOA1 listening (in SOAHOST1). SOAHOST2VHN is the virtual host name that maps to the virtual IP where WLS_SOA2 is listening (in SOAHOST2).

14.7.2 Specifying the Host Name Used by Oracle Coherence

Use the Administration Console to specify a host name used by Oracle Coherence.

To add the host name used by Oracle Coherence:

1. Log into the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**. The Summary of Servers page appears.
4. Click the name of the server (**WLS_SOA1** or **WLS_SOA2**, which are represented as hyperlinks) in Name column of the table. The settings page for the selected server appears.

5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Enter the following for WLS_SOA1 and WLS_SOA2 into the Arguments field.

For WLS_SOA1, enter the following:

```
-Dtangosol.coherence.wka1=SOAHOST1VHN  
-Dtangosol.coherence.wka2=SOAHOST2VHN  
-Dtangosol.coherence.localhost=SOAHOST1VHN
```

For WLS_SOA2, enter the following:

```
-Dtangosol.coherence.wka1=SOAHOST1VHN  
-Dtangosol.coherence.wka2=SOAHOST2VHN  
-Dtangosol.coherence.localhost=SOAHOST2VHN
```

Note: There should be no breaks in lines between the different -D parameters. Do not copy or paste the text to your Administration Console's arguments text field. It may result in HTML tags being inserted in the Java arguments. The text should not contain other text characters than those included the example above.

Note: The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) with the -Dtangosol.coherence.wkan.port and -Dtangosol.coherence.localport startup parameters. For example:

WLS_SOA1 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN  
-Dtangosol.coherence.wka2=SOAHOST2VHN  
-Dtangosol.coherence.localhost=SOAHOST1VHN  
-Dtangosol.coherence.localport=8089  
-Dtangosol.coherence.wka1.port=8089  
-Dtangosol.coherence.wka2.port=8089
```

WLS_SOA2 (enter the following into the Arguments field on a single line, without a carriage return):

```
-Dtangosol.coherence.wka1=SOAHOST1VHN  
-Dtangosol.coherence.wka2=SOAHOST2VHN  
-Dtangosol.coherence.localhost=SOAHOST2VHN  
-Dtangosol.coherence.localport=8089  
-Dtangosol.coherence.wka1.port=8089  
-Dtangosol.coherence.wka2.port=8089
```

For more information about Coherence Clusters see the *Oracle Coherence Developer's Guide*.

8. Click **Save and Activate Changes**.

Note: You must ensure that these variables are passed to the managed server correctly. (They should be reflected in the server's output log.) Failure of the Oracle Coherence framework can prevent the soa-infra application from starting.

Note: The multicast and unicast addresses are different from the ones used by the WebLogic Server cluster for cluster communication. SOA guarantees that composites are deployed to members of a single WebLogic Server cluster even though the communication protocol for the two entities (the WebLogic Server cluster and the groups to which composites are deployed) are different.

14.8 Post-Installation Steps on OIMHOST1

This section describes post-installation steps.

This section contains the following topics:

- [Section 14.8.1, "Starting the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1"](#)
- [Section 14.8.2, "Validating Oracle Identity Manager Instance on OIMHOST1"](#)

14.8.1 Starting the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1

Follow this sequence of steps to start the WLS_OIM1 and WLS_SOA1 Managed Servers on OIMHOST1:

1. Stop the WebLogic Administration Server on IDMHOST1 by using the WebLogic Administration Console as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Start the Administration Server on IDMHOST1 using the Node Manager, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
3. Validate that the Administration Server started up successfully by bringing up the Oracle WebLogic Administration Console.
4. Start NodeManager on OIMHOST1. Create the `nodemanager.properties` file by using the `startNodemanager.sh` script located under the `MW_HOME/wlserver_10.3/server/bin` directory.
5. Before you can start the Managed Servers by using the console, node manager requires that the property `StartScriptEnabled` be set to `true`. You set it by running the `setNMProps.sh` script located under the `MW_HOME/oracle_common/common/bin` directory.

`MW_HOME/oracle_common/common/bin/setNMProps.sh`
6. Restart the Node Manager as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components"](#) so that the properties take effect.
7. Start the WLS_SOA1 Managed Server, using the WebLogic Administration Console as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

8. Start the WLS_OIM1 Managed Server using the WebLogic Administration Console as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.8.2 Validating Oracle Identity Manager Instance on OIMHOST1

Validate the Oracle Identity Manager Server Instance by bringing up the Oracle Identity Manager Console in a web browser at:

`http://OIMHOST1VHN.mycompany.com:14000/oim`

Log in using the `xelsysadm` username and password.

Note: When you log in for the first time, you are prompted to setup Challenge Questions. Please do so before proceeding further.

Validate Oracle SOA Suite using the URL:

`http://SOAHOST1VHN.mycompany.com:8001/soa-infra`

Log in as the `weblogic` user.

14.9 Post-Installation Steps on OIMHOST2

It describes the post-installation steps on OIMHOST2.

This section contains the following topics:

- [Section 14.9.1, "Starting Node Manager on OIMHOST2"](#)
- [Section 14.9.2, "Starting the WLS_OIM2 and WLS_SOA2 Managed Servers on OIMHOST2"](#)
- [Section 14.9.3, "Validating Oracle Identity Manager Instance on OIMHOST2"](#)

14.9.1 Starting Node Manager on OIMHOST2

1. Start the Node Manager on OIMHOST2 to create the `nodemanager.properties` file by using the `startNodemanager.sh` script located under the `MW_HOME/wlserver_10.3/server/bin` directory.
2. Before you can start the Managed Servers by using the console, node manager requires that the property `StartScriptEnabled` is set to `true`. You set it by running the `setNMProps.sh` script located under the `MW_HOME/oracle_common/common/bin` directory.

```
cd MW_HOME/oracle_common/common/bin
./setNMProps.sh
```

3. Restart the Node Manager as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components"](#) so that the properties take effect.

14.9.2 Starting the WLS_OIM2 and WLS_SOA2 Managed Servers on OIMHOST2

Follow this sequence of steps to start the WLS_OIM2 Managed Server on OIMHOST2:

1. Start the WLS_SOA2 Managed Server, using the WebLogic Administration Console as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

2. Start the WLS_OIM2 Managed Server using the WebLogic Administration Console as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.9.3 Validating Oracle Identity Manager Instance on OIMHOST2

Validate the Oracle Identity Manager Server Instance by bringing up the Oracle Identity Manager Console in a web browser at:

`http://OIMHOST2VHN.mycompany.com:14000/oim/`

Log in using the xelsysadm username and password

Validate SOA at:

`http://SOAHOST2VHN.mycompany.com:8001/soa-infra`

Log in as the weblogic user.

14.10 Modifying the Oracle Identity Manager Properties to Support Active Directory

When first installed, Oracle Identity Manager has a set of default system properties for its operation.

If your Identity Store is in Active Directory, you must change the System property `XL.DefaultUserNamePolicyImpl` to `oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicyForAD` or `oracle.iam.identity.usermgmt.impl.plugins.LastNameFirstNamePolicyForAD`.

To learn how to do this, see the Administering System Properties chapter of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

14.11 Configuring Oracle Identity Manager to Reconcile from ID Store

In the current release, the `LDAPConfigPostSetup` script enables all the `LDAPSync`-related incremental Reconciliation Scheduler jobs, which are disabled by default. The LDAP configuration post-setup script is located under the `IAM_ORACLE_HOME/server/ldap_config_util` directory. Run the Script on `IDMHOST1`, as follows:

1. Edit the `ldapconfig.props` file located under the `IAM_ORACLE_HOME/server/ldap_config_util` directory and provide the following values:

Parameter	Value	Description
<code>OIMAdminUser</code>	<code>xelsysadm</code>	Oracle Identity Manager system administrator
<code>OIMProviderURL</code>	<code>t3://OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000</code>	List of Oracle Identity Manager managed servers.

Parameter	Value	Description
OIDURL	Specify the URL for the Oracle Internet Directory instance, for example: ldap://idstore.mycompany.com:389 ¹	Identity Store URL.
OIDAdminUsername	cn=oimLDAP,cn=systemids,dc=mycompany,dc=com	Name of use used to connect to Identity Store. This user should not be located in cn=Users,dc=mycompany,dc=com.
OIDSearchBase	dc=mycompany,dc=com	Root location in Identity Store where Users and Groups are located.
UserContainerName	cn=Users	cn of User location within Search base.
RoleContainerName	cn=Groups	cn of Groups location within Search base.
ReservationContainerName	cn=Reserve	cn of Reserve location within Search base.

¹ If you are using Oracle Internet Directory, Oracle Virtual Directory, or Active Directory, specify the appropriate URL

Note: usercontainerName, rolecontainername, and reservationcontainername are not used in this step.

2. Save the file.
3. Set the *JAVA_HOME* and *WL_HOME* environment variables.
4. Run LDAPConfigPostSetup.sh, providing the pathname to the ldapconfig.props file on the command line. The script prompts for the Oracle Identity Manager admin password. For example:

```
./LDAPConfigPostSetup.sh IAM_ORACLE_HOME/server/ldap_config_
util/ldapconfig.props
[Enter OIM admin password: ]
```

14.12 Configuring Oracle Identity Manager to Work with the Oracle Web Tier

This section describes how to configure Oracle Identity Manager to work with the Oracle Web Tier.

This section contains the following topics:

- [Section 14.12.1, "Prerequisites"](#)
- [Section 14.12.2, "Configuring Oracle HTTP Servers to Front End the Oracle Identity Manager and SOA Managed Servers"](#)
- [Section 14.12.3, "Changing Host Assertion in WebLogic"](#)
- [Section 14.12.4, "Validating Oracle Identity Manager Instance from the WebTier"](#)

- [Section 14.12.5, "Validating SOA Instance from the WebTier"](#)

14.12.1 Prerequisites

Before configuring Oracle Identity Manager to work with the Oracle Web Tier, ensure that the following tasks have been performed:

1. Install Oracle Web Tier on WEBHOST1 and WEBHOST2.
2. Configure the load balancer with a virtual host name (`sso.mycompany.com`) pointing to the web servers on WEBHOST1 and WEBHOST2.
3. Configure the load balancer with a virtual host name (`idminternal.mycompany.com`) pointing to the web servers on WEBHOST1 and WEBHOST2

14.12.2 Configuring Oracle HTTP Servers to Front End the Oracle Identity Manager and SOA Managed Servers

1. On each of the web servers on WEBHOST1 and WEBHOST2, edit the files `sso_vh.conf` and `idminternal_vh.conf`.

Add the following lines to the virtual host directive in `sso_vh.conf`:

```
# oim admin console(idmshell based)
<Location /admin>
    SetHandler weblogic-handler
    WProxySSL ON
    WProxySSLPassThrough ON
    WCookieName oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# oim self and advanced admin webapp consoles(canonic webapp)

<Location /oim>
    SetHandler weblogic-handler
    WProxySSL ON
    WProxySSLPassThrough ON
    WCookieName oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# xlWebApp - Legacy 9.x webapp (struts based)
<Location /xlWebApp>
    SetHandler weblogic-handler
    WProxySSL ON
    WProxySSLPassThrough ON
    WCookieName oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# Nexaweb WebApp - used for workflow designer and DM
<Location /Nexaweb>
```



```

        SetHandler weblogic-handler
        WProxySSL ON
        WProxySSLPassThrough ON
        WCookieName    oimjsessionid
        WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
        WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
    </Location>

# used for FA Callback service.
<Location /callbackResponseService>
    SetHandler weblogic-handler
    WProxySSL ON
    WProxySSLPassThrough ON
    WCookieName    oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# spml xsd profile
<Location /spml-xsd>
    SetHandler weblogic-handler
    WProxySSL ON
    WProxySSLPassThrough ON
    WCookieName    oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# role-sod profile
<Location /role-sod>
    SetHandler weblogic-handler
    WCookieName oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

<Location /HTTPClnt>
    SetHandler weblogic-handler
    WProxySSL ON
    WProxySSLPassThrough ON
    WCookieName    oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:1400
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

```

Add the following lines to the virtual host directive in `idminternal_vh.conf`:

```

# oim admin console(idmshell based)
<Location /admin>
    SetHandler weblogic-handler
    WCookieName    oimjsessionid
    WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
    WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

```

```
# oim self and advanced admin webapp consoles(canonic webapp)

<Location /oim>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>


# xlWebApp - Legacy 9.x webapp (struts based)
<Location /xlWebApp>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>


# Nexaweb WebApp - used for workflow designer and DM
<Location /Nexaweb>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>


# used for FA Callback service.
<Location /callbackResponseService>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>


# spml xsd profile
<Location /spml-xsd>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>


# role-sod profile
<Location /role-sod>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>


<Location /HTTPCInt>
  SetHandler weblogic-handler
  WLCookieName    oimjsessionid
  WebLogicCluster
```

```

OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# SOA Infrastructure
<Location /soa-infra>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicCluster SOAHOST1VHN:8001,SOAHOST2VHN:8001
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# UMS Email Support
<Location /ucs>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicCluster SOAHOST1VHN:8001,SOAHOST2VHN:8001
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# SOA Callback webservice for SOD - Provide the SOA Managed Server Ports
<Location /sodcheck>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicCluster SOAHOST1VHN:8001,SOAHOST2VHN:8001
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

# Callback webservice for SOA. SOA calls this when a request is
approved/rejected
# Provide the SOA Managed Server Port
<Location /workflowservice>
  SetHandler weblogic-handler
  WLCookieName oimjsessionid
  WebLogicCluster
OIMHOST1VHN.mycompany.com:14000,OIMHOST2VHN.mycompany.com:14000
  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/OHS/oim_component.log"
</Location>

```

Ensure that the newly added lines are within the VirtualHost directive, like this:

```

<VirtualHost *:7777>
  ServerName https://sso.mycompany.com:443
  ServerAdmin you@your.address
  ...

  -- added lines --
</VirtualHost>

```

2. Save the files on both WEBHOST1 and WEBHOST2.
3. Stop and start the Oracle HTTP Server instances on both WEBHOST1 and WEBHOST2 as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.12.3 Changing Host Assertion in WebLogic

Because the Oracle HTTP Server acts as a proxy for WebLogic, by default certain CGI environment variables are not passed through to WebLogic. These include the host

and port. You must tell WebLogic that it is using a virtual site name and port so that it can generate internal URLs appropriately.

To do this, log in to the WebLogic administration console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) Proceed as follows:

1. Select **Clusters** from the home page or, alternatively, select **Environment** -> **Clusters** from the **Domain** structure menu.
2. Click **Lock and Edit** in the Change Center Window to enable editing.
3. Click the **Cluster Name (soa_cluster)**.
4. In the **Configuration** tab, select the **HTTP** subtab.
Enter:
 - **Frontend Host:** `idminternal.mycompany.com`
 - **Frontend HTTP Port:** `80`
5. Click **Save**.
6. Click **Activate Changes** in the Change Center window to enable editing.
7. Restart WLS_SOA1 and WLS_SOA2 as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.12.4 Validating Oracle Identity Manager Instance from the WebTier

Validate the Oracle Identity Manager Server Instance by bringing up the Oracle Identity Manager Console in a web browser. at:

`https://sso.mycompany.com:443/oim`

Log in using the `xelsysadm` username and password.

14.12.5 Validating SOA Instance from the WebTier

Validate SOA by accessing the URL:

`http://idminternal.mycompany.com:80/soa-infra`

and logging in as the WebLogic administration user.

14.13 Configuring a Default Persistence Store for Transaction Recovery

The WLS_OIM and WLS_SOA Managed Servers have a transaction log that stores information about committed transactions that are coordinated by the server that might not have been completed. The WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

Note: Preferably, this location should be on a dual-ported SCSI disk or on a Storage Area Network (SAN).

Perform these steps to set the location for the default persistence stores for the Oracle Identity Manager and SOA Servers:

1. Create the following directories on the shared storage:

ORACLE_BASE/admin/domain_name/soa_cluster/tlogs

ORACLE_BASE/admin/domain_name/oim_cluster/tlogs

2. Log in to the Oracle WebLogic Server Administration Console.
3. Click **Lock and Edit**.
4. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.
The Summary of Servers page is displayed.
5. Click the name of either the Oracle Identity Manager or the SOA server (represented as a hyperlink) in the **Name** column of the table.
6. The Settings page for the selected server is displayed, and defaults to the **Configuration** tab.
7. Open the **Services** sub tab.
8. Under the **Default Store** section of the page, provide the path to the default persistent store on shared storage. The directory structure of the path is as follows:
 - For Oracle Identity Manager Servers: *ORACLE_BASE/admin/domain_name/oim_cluster/tlogs*
 - For SOA Servers: *ORACLE_BASE/admin/domain_name/soa_cluster/tlogs*

Note: To enable migration of the Transaction Recovery Service, specify a location on a persistent storage solution that is available to other servers in the cluster. All the servers that are a part of the cluster must be able to access this directory.

9. Click **Save and Activate**.
10. Restart the Oracle Identity Manager and SOA Managed Servers, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) to make the changes take effect.

14.14 Configuring an IT Resource Instance for Email

This section describes how to configure email notification. This is mandatory for Fusion Applications. The following steps assume that an email server has been set up and that Oracle Identity Management can use it to send the email notifications.

1. Log in to Oracle Identity Manager Advanced Administration as system administrator.
2. Navigate to **Configuration -> Create IT Resource**.
3. Enter *Email Server* for **IT Resource Name**. Select **Mail Server** for **IT Resource Type**. Do not select anything for the **Remote Manager** field. Click **Continue**.
4. On the **Step 2: Specify IT Resource Parameter Values** page, provide the following values for the fields:
 - **Authentication:** *False*
 - **Server Name:** *Email server name*, for example: *mail.mycompany.com*
User Login: leave blank

- **User Password:** leave blank
- Click **Continue**.
5. On the **Step 3: Set Access Permission to IT Resource** page, do not change anything. Click **Continue**.
 6. On the **Step 4: Verify IT Resource Details** page, check all the values you entered to verify that they are correct. Click **Continue**.
 7. On the **Step 5: IT Resource Connection Result** page, Oracle Identity Manager checks whether it can connect to the email server provided. If the connection is successful, click **Create**.
 8. On the **Step 6: IT Resource Created** page, click **Finish**.
 9. Restart the Oracle Identity Manager server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) for the changes to take effect.

14.15 Enabling Oracle Identity Manager to Connect to SOA Using the Administrative Users Provisioned in LDAP

Oracle Identity Manager connects to SOA as SOA administrator, with the username `weblogic` by default. As mentioned in the previous sections, a new administrator user is provisioned in the central LDAP store to manage Identity Management Weblogic Domain.

Perform the following postinstallation steps to enable Oracle Identity Manager to work with the Oracle WebLogic Server administrator user provisioned in the central LDAP store. This enables Oracle Identity Manager to connect to SOA without any problem:

1. Log in to Enterprise Manager at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. For a single domain topology, select **Farm_IDMDomain** → **Identity and Access** → **OIM** → **oim(11.1.1.3.0)**.
For a split domain topology, select **Farm_OIMDomain** → **Identity and Access** → **OIM** → **oim(11.1.1.3.0)**.
3. Select **MBean Browser** from the menu or right click to select it.
4. Select **Application defined Mbeans** → **oracle.iam** → **Server: wls_oim1** → **Application: oim** → **XML Config** → **Config** → **XMLConfig.SOAConfig** → **SOAConfig**
5. Change the **username** attribute to the Oracle WebLogic Server administrator username provisioned in [Section 11.5, "Preparing the Identity Store,"](#) for example: `weblogic_idm`.
Change **SOA Config RMI URL** to:
`t3://SOAHOST1VHN:8001, SOAHOST2VHN:8001`
6. Click **Apply**.
7. For a single domain topology, select **Weblogic Domain** → **IDMDomain** from the Navigator.
For a split domain topology, select **Weblogic Domain** → **OIMDomain**
8. Select **Security** → **Credentials** from the down menu.

9. Expand the key **oim**.
10. Click **SOAAdminPassword**.
11. Click **Edit**.
12. Change the username to `weblogic_idm` and set the password to the accounts password.
13. Click **OK**.
14. Run the reconciliation process to enable the Oracle WebLogic Server administrator, `weblogic_idm`, to be visible in the OIM Console. Follow these steps:
 - a. Log in to Oracle Identity Manager at:
`https://sso.mycompany.com:443/oim` as the user `xelsysadm`.
 - b. If prompted, set up challenge questions. This happens on your first login to Oracle Identity Manager.
 - c. Click **Advanced**.
 - d. Click the **System Management** tab.
 - e. Click the arrow for the **Search Scheduled Jobs** to list all the schedulers.
 - f. Select **LDAP User Create and Update Full Reconciliation**.
 - g. Click **Run Now** to run the job.
 - h. Go to the Administration page and perform a search to verify that the user is visible in the Oracle Identity Manager console.
15. Select **Administration**.
16. Click **Advanced Search -> Roles**
17. Search for the Administrators role.
18. Click the **Administrators Role**.
19. Click **Open**.
20. Click the **Members** tab.
21. Click **Assign**.
22. Type `weblogic_idm` in the Search box and Click **->**.
23. Select **weblogic_idm** from the list of available users.
24. Click **>** to move to **Selected Users**.
25. Click **Save**.
26. Restart Oracle Identity Manager managed server.

14.16 Updating the Username Generation Policy for Active Directory

If your back end directory is Active Directory, you must update Oracle Identity Manager so that it only allows user names with a maximum of 20 characters. This is a limitation of Active Directory. Update the username generation policy from `DefaultComboPolicy` to `FirstnameLastnamepolicyforAD` as follows.

1. Log in to the OIM Console at the URL listed in [Section 14.2, "About Domain URLs."](#)

2. Click **Advanced** on the top of the right pane.
3. Click **Search System properties**.
4. On the navigation bar in the left pane, search on **Username Generation**.
5. Click **Default Policy for Username Generation**.
6. In the **Value** field, update the entry from
`oracle.iam.identity.usermgmt.impl.plugins.DefaultComboPolicy`
to
`oracle.iam.identity.usermgmt.impl.plugins.FirstNameLastNamePolicyForAD`.
7. Click **Save**.

14.17 Tuning Oracle Platform Security

In order for Oracle Platform Security to work optimally, add tuning parameters to managed servers when they start. In particular, provide these values to the following managed servers:

- Admin Server
- WLS_OAM1
- WLS_OAM2
- WLS_OIM1
- WLS_OIM2

To add these values to the server start parameters perform the following steps.

1. Log in to the weblogic console using at:
`http://admin.mycompany.com/console`
2. Click **Lock and Edit**.
3. Expand the **Environment** Node in the Domain Structure window.
4. Click **Servers** to open the Summary of Servers Page.
5. Click on a server to show the server properties page.
6. Click the **Server Start** tab.
7. Add the following values to the **Arguments** field:
 - `-Djps.subject.cache.key=5`
 - `-Djps.subject.cache.ttl=600000`.
8. Click **Save**.
9. Repeat for each of the managed servers.
10. Click **Activate Changes**.

For information about tuning OPSS, see the "Oracle Fusion Middleware Security Performance Tuning" chapter in the *Oracle Fusion Middleware Performance and Tuning Guide*.

14.18 Provisioning Users to the Enterprise Identity Store in a Multidirectory Scenario

This section provides details for configuring Oracle Identity Manager to provision users in the enterprise identity store. It contains the following topics:

- [Section 14.18.1, "Creating and Importing New Rules."](#)
- [Section 14.18.2, "Updating IT Resource for Oracle Identity Manager Integration."](#)
- [Section 14.18.3, "Updating the Incremental Reconciliation Changelog Number."](#)

By default, the users created from Fusion Applications are provisioned in the Enterprise Identity Store. You can also configure the users to be created in the shadow directory by configuring the Oracle Identity Manager rules appropriately.

14.18.1 Creating and Importing New Rules

1. Create `LDAPContainerRules.xml` with the new rules that you want to import into LDAP. This file contains the rules for user creation and role creation and corresponding containers in LDAP where they should be created. For the current split profile environment, the rules are:

```
<?xml version='1.0' encoding='UTF-8'?>
<container-rules>
  <user>
    <rule>
      <expression>Country=IN</expression>
      <container>cn=Users,dc=idm,dc=sun,dc=com</container>
    </rule>
    <rule>
      <expression>Default</expression>
      <container>cn=Users,dc=mycompany,dc=com</container>
      <description>UserContainer</description>
    </rule>
  </user>
  <role>
    <rule>
      <expression>Default</expression>
      <container>cn=Groups,dc=mycompany,dc=com</container>
      <description>RoleContainer</description>
    </rule>
  </role>
</container-rules>
```

2. Import this configuration to MDS.

Modify the `weblogic.properties` file under `OIM_ORACLE_HOME/bin` as follows.

```
wls_servername=OIM server name
```

For example, `WLS_OIM1`.

Note: This is only used to load the data, so it is only necessary to specify one Oracle Identity Manager server.

```
application_name=OIMMetadata
metadata_from_loc = /u01/tmp
```

```
metadata_files=/db/LDAPContainerRules.xml
```

3. Set the `OIM_ORACLE_HOME` environment variable to the appropriate directory.
4. Run the following command to import the configuration file into MDS. The file `weblogicImportMetadata.sh` is located under `OIM_ORACLE_HOME/bin`

```
sh ./weblogicImportMetadata.sh

Please enter your username [weblogic] :weblogic
Please enter your password [weblogic] :Weblogic user password
Please enter your server URL [t3://localhost:7001
:t3://ADMINVHN.mycompany.com:7001
```
5. To activate the new rules, restart the Oracle Identity Manager Servers `wls_oim1` and `wls_oim2` as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

14.18.2 Updating IT Resource for Oracle Identity Manager Integration

Using the Oracle Identity Manager advanced console, update the directory server IT resource with Oracle Virtual Directory information. The steps are as follows:

1. Log in to the OIM Console at:

```
https://sso.mycompany.com:443/oim
```
2. Click **Advanced** to go to the advanced console.
3. On the advanced console page, in the Configuration section, click the link for **Manage IT Resource**. The Manage IT Resource window appears.
4. In the Manage IT Resource window, under **IT Resource Type**, choose **Directory Server**, then click **Search**.
5. In the resulting list of resources in the IT Resource Name section, choose the **Directory Server** link for that instance's information. The View IT Resource window appears.
6. Click **Edit** in the View IT Resource window and enter your LDAP server information.
 - Admin Login: Bind dn to connect to the Oracle Virtual Directory server
 - Admin Password: Bind password to connect to the Oracle Virtual Directory server
 - Search Base: LDAP Container (*DefaultNamingContext*) for all users and groups
 - Server URL: Oracle Virtual Directory host and port,

```
ldap://IDMHOST1.mycompany.com:389
```
 - Server SSL URL:

```
ldaps://IDMHOST1.mycompany.com:636
```
 - User Reservation Container: Container used for reserving user id, for example:

```
cn=reserve,dc=mycompany,dc=com
```
7. Click **Update** and close the window.

14.18.3 Updating the Incremental Reconciliation Changelog Number

Whenever the environment is initially set up as a non-split profile and then converted to a split profile, some incremental jobs were run before the conversion. As a result, the

last changelog number field is not in a format that the split profile environment can decipher. This results in all subsequent incremental jobs failing with the error message:

```
Failed:oracle.iam.scheduler.exception.RequiredParameterNotSetException: The value
is not supported.
```

To resolve the error, you must update the last changelog number needs to 0, as follows:

1. Log in to the OIM Console at:
`https://sso.mycompany.com:443/oim`
2. Click **Advanced** on the top right pane.
3. Click **Search Scheduled Jobs**.
4. On the navigation bar in the left pane, perform a search on LDAP*.
5. Click **LDAP User Create and Update Reconciliation Job**.
6. Update the last change number to 0.
7. Click **Apply**.
8. Click **Run Now**.

Repeat Steps 1-11 for all the incremental reconciliation jobs:

- LDAP Role Create and Update Reconciliation
- LDAP Role Membership Reconciliation
- LDAP Role Hierarchy Reconciliation
- LDAP User Delete Reconciliation
- LDAP Role Delete Reconciliation

14.19 Excluding Users from Oracle Identity Manager Reconciliation

By default Oracle Identity Management reconciles all users that are located in the LDAP container `cn=Users`. Once reconciled, these users are subject to the usual password ageing policies defined in Oracle Identity Manager. This is not desirable for system accounts. It is recommended that you exclude the following accounts from this reconciliation:

- `xelsysadm`
- `oimLDAP`
- `oamLDAP`

Additionally, you might want to exclude:

- `IDROUser`
- `IDRWUser`
- `PolicyROUser`
- `PolicyRWUser`

To exclude these users from reconciliation and discard failed reconciliation events, perform the following steps, using ODSM and the OIM Console:

14.19.1 Adding the orclAppIDUser Object Class to the User by Using ODSM

1. Log in to ODSM at:
`http://admin.mycompany.com/odsm`
2. Connect to one of the LDAP instances that hosts the user to be excluded.
3. Select **Data Browser**.
4. Enter the user name in the query box and execute the search.
5. Click on the user to bring up the Edit window.
6. Click **Attributes**.
7. Click **+** in the Object Classes box to add a new class.
8. Enter `orclAppIDUser` in the search box and execute the search.
9. Click on the attribute `orclAppIDUser` and click **OK**.
10. Click **Apply**.

Repeat Steps 1-10 for each user to be excluded.

14.19.2 Closing Failed Reconciliation Events by Using the OIM Console

1. Log in to the OIM Console as the `xelsysadm` user, using the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click **Advanced**.
3. From Event Management, select **Search Reconciliation Events**.
4. Click **Advanced Search**.
5. In the **Current Status** field, select **Equals**. In the **Search** box, select **Creation Failed** from the list.
6. Click **Search**.
7. Select each of the events.
8. From the Actions menu, select **Close Event**.
9. In the Confirmation window enter a justification, such as `Close Failed Reconciliation Events`.
10. Click **Closed**.
11. Click **OK** to acknowledge the confirmation message.

14.20 Backing Up the Application Tier Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the web tier as described in [Section 7.6, "Backing up the Web Tier Configuration."](#)
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.
3. Back up the Administration Server domain directory as described in [Section 8.10, "Backing Up the WebLogic Domain."](#)
4. Back up the Oracle Internet Directory as described in [Section 9.8, "Backing up the Oracle Internet Directory Configuration."](#)
5. Back up the Oracle Virtual Directory as described in [Section 12.9, "Backing Up the Oracle Virtual Directory Configuration."](#)

For information about backing up the application tier configuration, see [Section 20.6, "Performing Backups and Recoveries."](#)

Extending the Domain to Include Oracle Identity Federation

This chapter describes how to extend the Identity Management domain to include Oracle Identity Federation in an enterprise deployment.

Installing Oracle Identity Federation is optional. You should only perform the steps in this chapter if you intend to use Oracle Identity Federation. This chapter sets up Oracle Identity Federation in Service Provider (SP) mode. Note that the steps in this chapter are complete only with respect to configuring Oracle Identity and Access Management.

You must fully configure your Identification Provider (IP) before you switch on Federation in [Section 18.4.3, "Switching from Local Authentication to Federation SSO."](#) The steps to configure your IP are outside the scope of this document.

This chapter contains the following topics:

- [Section 15.1, "Overview of Extending the Domain to Include Oracle Identity Federation"](#)
- [Section 15.2, "Prerequisites"](#)
- [Section 15.3, "Configuring Oracle Identity Federation on IDMHOST1"](#)
- [Section 15.5, "Configuring Oracle Identity Federation on IDMHOST2"](#)
- [Section 15.6, "Provisioning the Managed Servers on the Local Disk"](#)
- [Section 15.7, "Validating Oracle Identity Federation"](#)
- [Section 15.8, "Configure the Enterprise Manager Agents"](#)
- [Section 15.9, "Enabling Oracle Identity Federation Integration with LDAP Servers"](#)
- [Section 15.10, "Configuring Oracle Identity Federation to work with the Oracle Web Tier"](#)
- [Section 15.11, "Validating Oracle Identity Federation"](#)
- [Section 15.12, "Backing Up the Application Tier Configuration"](#)

15.1 Overview of Extending the Domain to Include Oracle Identity Federation

Oracle Identity Federation is a self-contained, standalone federation server that enables single sign-on and authentication in a multiple-domain identity network and supports the broadest set of federation standards. This enables users to federate in

heterogeneous environments and business associations, whether they have implemented other Oracle Identity Management products in their solution set or not.

15.2 Prerequisites

Before proceeding with Oracle Identity Federation configuration, ensure that you have done the following.

1. Install and upgrade the software on IDMHOST1 and IDMHOST2 as described in [Section 6.3.3, "Installing Oracle WebLogic Server and Creating the Fusion Middleware Home"](#) and [Section 6.3.4, "Installing Oracle Identity Management."](#)
2. Run the Repository Creation Utility (RCU) to create and configure the collection of schemas used by Oracle Identity Federation as described in [Chapter 5, "Preparing the Database for an Enterprise Deployment."](#)
3. Create the Identity Management domain as described in [Chapter 8, "Creating Domains for an Enterprise Deployment."](#)
4. Install and configure Oracle Internet Directory as described in [Chapter 9, "Extending the Domain to Include Oracle Internet Directory."](#) Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory is used as the User Store and the Federation Store
5. Install and configure Oracle HTTP Server on WEBHOST1 and WEBHOST2 as described in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment."](#)
6. Associate the Identity Management domain created with an External LDAP Store as described in [Section 11.4.2, "Reassociating the Policy and Credential Store."](#) This is required because Oracle Identity Federation is being extended on a node where the Administration Server is not running.

15.3 Configuring Oracle Identity Federation on IDMHOST1

Ensure that the system, patch, kernel and other requirements are met. These are listed in the Oracle Fusion Middleware Installation Guide for Oracle Identity Management manual in the Oracle Fusion Middleware documentation library for the platform and version you are using.

If you plan on provisioning the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 4.4.4, "Directory Structure."](#)

On UNIX:

1. Ensure that port 7499 is not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

```
netstat -an | grep "7499"
```

If the port is in use (if the command returns output identifying the port), you must free it.

On UNIX:

Remove the entries for port 7499 in the `/etc/services` file and restart the services, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

2. Create a file containing the ports used by Oracle Internet Directory. On Disk1 of the installation media, locate the file `stage/Response/staticports.ini`. Copy it to a file called `oif_ports.ini`. Delete all entries in `oif_ports.ini` except for Oracle Identity Federation Server Port. Change the value of that port to 7499.

Note: If the port name in the file is slightly different from those listed in this step, use the name in the file.

3. Start the Oracle Identity Management 11g Configuration Wizard located under the `IDM_ORACLE_HOME/bin` directory as follows:

On UNIX, issue this command:

```
./config.sh
```

On Windows, double-click `config.exe`

4. On the Welcome screen, click **Next**.
5. On the Select Domain screen, select Extend Existing Domain and specify these values:
 - **HostName:** `adminvhn.mycompany.com`
 - **Port:** 7001
 - **UserName:** `weblogic`
 - **User Password:** `weblogic_user_password`

Click **Next**.

6. A dialog box with the following message appears:

The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer to the Identity Management documentation for information on how to verify the domain is valid.

This is a benign warning that you can ignore.

Click **Yes** to continue.

7. On the Specify Installation Location screen, specify the following values:
 - **Oracle Middleware Home Location:** `/u01/app/oracle/product/fmw`
This value is prefilled and cannot be updated.
 - **Oracle Home Directory:** `idm`
This value is prefilled and cannot be updated
 - **WebLogic Server Directory:**
`/u01/app/oracle/product/fmw/wlserver_10.3`
 - **Oracle Instance Location:** `/u01/app/oracle/admin/instances/oif_inst1`
 - **Instance Name:** `oif_inst1`

Click **Next**.

8. On the Specify Security Updates screen (if shown), specify the values shown in this example:
 - **Email Address:** Provide the email address for your My Oracle Support account.
 - **Oracle Support Password:** Provide the password for your My Oracle Support account.
 - Select **I wish to receive security updates via My Oracle Support**.Click **Next**.
9. On the Configure Components screen, de-select all the components except Oracle Identity Federation components. Select only Oracle Identity Federation from the Oracle Identity Federation components. Do not select Oracle HTTP Server. Select **Clustered**.
Click **Next**.
10. On the Configure Ports screen, you use the `oif_ports.ini` file you created in Step 2 to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `oif_ports.ini`.
 - c. Click **Save**, then click **Next**.
11. On the Specify OIF Details screen, specify these values:
 - **PKCS12 Password:** `password`
 - **Confirm Password:** Confirm the password
 - **Server Id:** `WLS_OIF1`Click **Next**.
12. On the Select OIF Advanced Flow Attributes screen, specify these values:
 - **Authentication Type:** `LDAP`
 - **User Store:** `LDAP`
 - **Federation Store:** `RDBMS`
 - **User Session Store:** `RDBMS` (default selection, which cannot be changed for a cluster)
 - **Message Store:** `RDBMS` (default selection, which cannot be changed for a cluster)
 - **Configuration Store:** `RDBMS` (default selection, which cannot be changed for a cluster)

Note: When you choose `RDBMS` for the session, message, and configuration data stores during an Advanced installation, the installer creates one data source for all three data stores. If you want to have separate databases for each of these stores, you must configure this after the installation by using the OUI Config Wizard.

Click **Next**.

13. On the Authentication LDAP Details screen, specify the following values:

- **LDAP Type:** Select **Oracle Internet Directory** if you have an Oracle Internet Directory only topology without Oracle Virtual Directory. Otherwise select Oracle Virtual Directory.
- **LDAP URL:** The LDAP URL to connect to your LDAP store in the format: `ldaps://host:port`. For example:
`ldaps://idstore.mycompany.com:636`
- **LDAP Bind DN:** `cn=orcladmin`
- **LDAP Password:** `orcladmin_password`
- **User Credential ID Attribute:** `uid`
- **User Unique ID Attribute:** `uid`
- **Person Object Class:** `inetOrgPerson`
- **Base DN:** `dc=mycompany,dc=com`

Click Next.

14. On the LDAP Attributes for User Data Store screen, specify the following values:

- **LDAP Type:** Select **Oracle Internet Directory** if you have an Oracle Internet Directory only topology without Oracle Virtual Directory. Otherwise select **Oracle Virtual Directory**.
- **LDAP URL:** The LDAP URL to connect to your LDAP store in the format: `ldaps://host:port`. For example:
`ldaps://idstore.mycompany.com:636`
- **LDAP Bind DN:** `cn=orcladmin`
- **LDAP Password:** `orcladmin_password`
- **User Description Attribute:** `uid`
- **User ID Attribute:** `uid`
- **Person Object Class:** `inetOrgPerson`
- **Base DN:** `dc=mycompany,dc=com`

Click Next.

15. On the Specify Federation Store Database Details screen, specify the following values.

- **Host Name:** The connect string to your database. For example:
`idmdbhost1-vip.mycompany.com:1521: idmdb1^idmdbhost2-vip.mycompany.com:1521: idmdb2@oifedg.mycompany.com`

Notes:

- The Oracle RAC database connect string information must be provided in the format:
host1:port1:instance1^host2:port2:instance2@service_name
 - During this installation, it is not required for all the Oracle RAC instances to be up. If one Oracle RAC instance is up, the installation can proceed.
 - It is required that the information provided is complete and accurate. Specifically, the correct host, port, and instance name must be provided for each Oracle RAC instance, and the service name provided must be configured for all the specified Oracle RAC instances.

Any incorrect information entered in the Oracle RAC database connect string has to be corrected manually after the installation.
 - If you are using Oracle Database 11.2, replace the vip address and port with the 11.2 SCAN address and port.
-

- **UserName:** The username for the OIF Schema. For example: `edg_oif`
- **Password:** `oif_user_password`

Click **Next**.

16. On the Transient Store Database Details screen, specify the values shown in this example:

- **Host Name:** The connect string to your database. For example:
`idmdbhost1-vip.mycompany.com:1521:idmdb1^idmdbhost2-vip.mycompany.com:1521:idmdb2@oifedg.mycompany.com`
- **UserName:** The username for the OIF Schema. For example: `edg_oif`
- **Password:** `oif_user_password`

Click **Next**.

17. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not correct, click **Back** to modify selections on previous screens. Then click **Configure**.
18. On the Configuration Progress screen, view the progress of the configuration.
19. On the Configuration Complete screen, click **Finish** to confirm your choice to exit.

15.4 Run Upgrade Script

Run the `oif-upgrade-11.1.1.2.0-11.1.1.6.0.py` script as described in "Updating Configuration Properties in Oracle Identity Federation" in *Oracle Fusion Middleware Patching Guide*.

15.5 Configuring Oracle Identity Federation on IDMHOST2

1. Ensure that the system, patch, kernel and other requirements are met. These are listed in the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management* in the Oracle Fusion Middleware documentation library for the platform and version you are using.
2. If you plan to provision the Instance Home or the Managed Server domain directory on shared storage, ensure that the appropriate shared storage volumes are mounted on IDMHOST1 as described in [Section 4.4.4, "Directory Structure."](#)
3. Ensure that port 7499 is not in use by any service on the computer by issuing these commands for the operating system you are using. If a port is not in use, no output is returned from the command.

On UNIX:

```
netstat -an | grep "7499"
```

If the port is in use (if the command returns output identifying the port), you must free it.

On UNIX:

Remove the entries for port 7499 in the `/etc/services` file and restart the services, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) or restart the computer.

4. Start the Oracle Identity Management 11g Configuration Wizard located under the `IDM_ORACLE_HOME/bin` directory as follows:

On UNIX, issue this command:

```
./config.sh
```

On Windows, double-click `config.exe`

5. On the Welcome screen, click **Next**.
6. On the Select Domain screen, select the **Expand Cluster** option and specify these values:
 - **HostName:** `ADMINVHN.mycompany.com`
 - **Port:** `7001`
 - **UserName:** `weblogic`
 - **User Password:** `weblogic_user_password`

Click **Next**.

7. A dialog box with the following message appears:

The selected domain is not a valid Identity Management domain or the installer cannot determine if it is a valid domain. If you created the domain using the Identity Management installer, you can ignore this message and continue. If you did not create the domain using the Identity Management installer, refer to the Identity Management documentation for information on how to verify the domain is valid.

This is a benign warning that you can ignore.

Click **Yes** to continue.

8. On the Specify Installation Location screen, specify the following values:

- **Oracle Middleware Home Location:** `/u01/app/oracle/product/fmw`
(This value is prefilled and cannot be updated.)
 - **Oracle Home Directory:** `idm` (This value is prefilled and cannot be updated.)
 - **WebLogic Server Directory:**
`/u01/app/oracle/product/fmw/wlserver_10.3`
 - **Oracle Instance Location:** `/u01/app/oracle/admin/instances/oif_inst2`
 - **Instance Name:** `oif_inst2`
- Click **Next**.
9. On the Specify Security Updates screen (if shown), specify the values shown in this example:
 - **Email Address:** Provide the email address for your My Oracle Support account.
 - **Oracle Support Password:** Provide the password for your My Oracle Support account.
 - Select **I wish to receive security updates via My Oracle Support**.Click **Next**.
 10. On the Configure Components screen, de-select all the components except Oracle Identity Federation components. Select only Oracle Identity Federation from the Oracle Identity Federation components. Do not select Oracle HTTP Server.
Click **Next**.
 11. On the Configure Ports screen, you use the `oif_ports.ini` file you created in [Section 15.3, "Configuring Oracle Identity Federation on IDMHOST1"](#) to specify the ports to be used. This enables you to bypass automatic port configuration.
 - a. Select **Specify Ports using a Configuration File**.
 - b. In the file name field specify `oif_ports.ini`.
 - c. Click **Save**, then click **Next**.
 12. On the Installation Summary screen, review the selections to ensure that they are correct. If they are not correct, click **Back** to modify selections on previous screens. Then click **Configure**.
 13. On the Configuration Progress screen, view the progress of the configuration.
 14. On the Installation Complete screen, click **Finish** to confirm your choice to exit.

15.6 Provisioning the Managed Servers on the Local Disk

Due to certain limitations, the Oracle Configuration Wizard creates the domain configuration under the Identity Management Oracle home. In this deployment guide, the Oracle home is on shared disk and it is a best practice recommendation to separate the domain configuration from the Oracle home. This section provides the steps to separate the domain. Proceed as follows:

1. From IDMHOST1, copy the applications directory under the `MW_HOME/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_oif1` directory to the `MW_HOME/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_oif2` directory.

```
cp -rp MW_HOME/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_oif1/applications user@IDMHOST1:/ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain/config/fmwconfig/servers/wls_oif2/
```

2. On IDMHOST1, pack the Managed Server domain using the pack command located under the `ORACLE_COMMON_HOME/common/bin` directory. Make sure to pass the `-managed=true` flag to pack the Managed Server. Type:

```
ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true \
-domain=path_to_adminServer_domain -template=templateName.jar \
-template_name=templateName
```

For example

```
ORACLE_COMMON_HOME/common/bin/pack.sh -managed=true \
-domain=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain \
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
-template_name=ManagedServer_Template
```

3. Copy the Managed Server template directory from IDMHOST1 to IDMHOST2. For Example:

```
scp -rp /u01/app/oracle/products/fmw/templates
user@IDMHOST2:/u01/app/oracle/products/fmw/templates
```

4. Unpack the Managed Server to the local disk on IDMHOST1 using the unpack command located under the `ORACLE_COMMON_HOME/common/bin` directory.

```
ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
-template=templateName.jar -app_dir=path_to_appdir_on_localdisk \
-overwrite_domain=true
```

For example:

```
ORACLE_COMMON_HOME/common/bin/unpack.sh \
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
-app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications \
-overwrite_domain=true
```

5. Unpack the Managed Server to the local disk on IDMHOST2 using the unpack command located under the `ORACLE_COMMON_HOME/bin` directory.

```
ORACLE_COMMON_HOME/common/bin/unpack.sh -domain=path_to_domain_on_localdisk \
-template=templateName.jar -app_dir=path_to_appdir_on_localdisk \
-overwrite_domain=true
```

For example:

```
ORACLE_COMMON_HOME/common/bin/unpack.sh \
-domain=/u01/app/oracle/admin/IDMDomain/mserver/IDMDomain \
-template=/u01/app/oracle/product/fmw/templates/managedServer.jar \
-app_dir=/u01/app/oracle/admin/IDMDomain/mserver/applications \
-overwrite_domain=true
```

6. Restart the Administration server by following the steps in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
7. Validate that the Administration Server started up successfully by opening a browser accessing the Administration Console at `http://ADMINVHN.mycompany.com:7001/console`.

Also validate Enterprise Manager by opening a browser and accessing Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`.

8. Restart the Managed Servers WLS_OIF1 and WLS_OIF2 as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

15.7 Validating Oracle Identity Federation

Validate the configuration of Oracle Identity Federation on IDMHOST1 and IDMHOST2 by accessing the SP metadata on each host.

On IDMHOST1, access the SP metadata by going to:

`http://idmhost1.mycompany.com:7499/fed/sp/metadata`

On IDMHOST2, access the SP metadata by going to:

`http://idmhost2.mycompany.com:7499/fed/sp/metadata`

15.8 Configure the Enterprise Manager Agents

All the Oracle Fusion Middleware components deployed in this enterprise deployment are managed by using Oracle Enterprise Manager Fusion Middleware Control. To manage Oracle Identity Federation with this tool, you must configure the EM agents with the correct monitoring credentials. Update the credentials for the EM agents associated with IDMHOST1 and IDMHOST2. Follow these steps to complete this task:

1. Use a web browser to access Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN.mycompany.com:7001/em`. Log in as the WebLogic user.
2. From the Domain Home Page, navigate to the Agent-Monitored Targets page using the menu under **Farm -> Agent-Monitored Targets**.
 - Click the **Configure** link for the Target Type Identity Federation Server to go to the Configure Target Page.
 - On the Configure Target Page, click **Change Agent** and choose the correct agent for the host.
 - Update the **WebLogic monitoring user name** and the **WebLogic monitoring password**. Enter `weblogic` as the WebLogic monitoring user name and the password for the weblogic user as the WebLogic monitoring password.
 - Click **OK** to save your changes.

15.9 Enabling Oracle Identity Federation Integration with LDAP Servers

By default, Oracle Identity Federation is not configured to be integrated with LDAP Servers deployed in a high availability configuration. To integrate Oracle Identity Federation with highly available LDAP Servers to serve as user data store, federation data store, or authentication engine, you must configure Oracle Identity Federation based on the LDAP server's function.

Proceed as follows to integrate Oracle Identity Federation with an LDAP Server deployed in a high availability configuration

1. On IDMHOST1, set the `DOMAIN_HOME` and `IDM_ORACLE_HOME` environment variables.

2. On IDMHOST1, set the environment using the `setOIFEnv.sh` script. This script is located under the `IDM_ORACLE_HOME/fed/scripts` directory.

For example:

```
export DOMAIN_HOME=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain
export IDM_ORACLE_HOME=IDM_ORACLE_HOME
cd $IDM_ORACLE_HOME/fed/scripts
. setOIFEnv.sh
```

3. On IDMHOST1, run the `WLST` script located under the `ORACLE_COMMON_HOME/bin` directory.

```
cd ORACLE_COMMON_HOME/common/bin
./wlst.sh
```

4. Connect to one of the Oracle Identity Federation Managed Servers:

```
connect()
```

Enter the username and password to connect to the Oracle Identity Federation Managed Servers. This is the same as the WebLogic Administration user name and password.

Enter the URL to connect to the Oracle Identity Federation Managed Server:

```
t3://IDMHOST1.mycompany.com:7499
```

5. Then enter the following properties, as needed:

- To integrate the user data store with a highly available LDAP Server, set the `userldaphaenabled` boolean property from the `datastore` group to `true`:

```
setConfigProperty('datastore','userldaphaenabled', 'true', 'boolean')
Update was successful for: userldaphaenabled
```

- Validate the user data store is integrated with a highly available LDAP store by running:

```
getConfigProperty('datastore', 'userldaphaenabled')
Value(s) for property: true
```

The `userldaphaenabled` property must return `true`.

- To integrate the LDAP authentication engine with a highly available LDAP Server, set the `ldaphaenabled` boolean property from the `authnengines` group to `true`:

```
setConfigProperty('authnengines','ldaphaenabled', 'true', 'boolean')
Update was successful for: ldaphaenabled
```

- Validate the LDAP authentication engine is integrated with a highly available LDAP store by running:

```
getConfigProperty('authnengines','ldaphaenabled')
Value(s) for property: true
```

The `ldaphaenabled` property for the `authnengines` group must return `true`.

Note: On IDMHOST1, delete the following directories:

- `ORACLE_`
`BASE/admin/IDMDomain/aserver/IDMDomain/config/fmw`
`config/servers/wls_oif1/applications`
 - `ORACLE_`
`BASE/admin/IDMDomain/aserver/IDMDomain/config/fmw`
`config/servers/wls_oif2/applications`
-
-

15.10 Configuring Oracle Identity Federation to work with the Oracle Web Tier

This section describes how to configure Oracle Access Manager to work with the Oracle Web Tier.

This section contains the following topics:

- [Section 15.10.1, "Prerequisites"](#)
- [Section 15.10.2, "Making Oracle Identity Federation aware of the Load Balancer"](#)
- [Section 15.10.3, "Configuring Oracle HTTP Servers To Front End the Oracle Identity Federation Managed Servers"](#)

15.10.1 Prerequisites

Before proceeding, ensure that the following tasks have been performed:

1. Oracle Web Tier has been installed on WEBHOST1 and WEBHOST2.
2. Oracle Access Manager has been installed and configured on IDMHOST1 and IDMHOST2.
3. The load balancer has been configured with a virtual host name (`sso.mycompany.com`) pointing to the web servers on WEBHOST1 and WEBHOST2.
4. The load balancer has been configured with a virtual host name (`admin.mycompany.com`) pointing to web servers WEBHOST1 and WEBHOST2.

15.10.2 Making Oracle Identity Federation aware of the Load Balancer

To configure the Oracle Identity Federation application to use the load balancer VIP, follow these steps:

1. Log in to the Oracle Enterprise Manager Fusion Middleware Control console using the credentials of the Administrative user (for example: `weblogic`).
2. Navigate to an OIF node in Oracle Enterprise Manager Fusion Middleware Control. the OIF nodes are under **Identity and Access** in the navigation tree.
3. From the **OIF** menu, select **Administration**, and then **Server Properties**.

Change the host name to `sso.mycompany.com` and the port to 443.

Select **SSL Enabled**.

Click **Apply**.

4. From the **OIF** menu in Oracle Enterprise Manager Fusion Middleware Control, select **Administration**, and then **Service Provider**.

Change the URL to `https://sso.mycompany.com:443/fed/sp`.

Click **Apply**.

15.10.3 Configuring Oracle HTTP Servers To Front End the Oracle Identity Federation Managed Servers

On each of the web servers on WEBHOST1 and WEBHOST2, edit the file called `sso_vh.conf` in the directory `ORACLE_INSTANCE/config/OHS/component/moduleconf`. Add the following lines:

```
<Location /fed>
  SetHandler weblogic-handler
  WLProxySSL ON
  WLProxySSLPassThrough ON
  WebLogicCluster idmhost1.mycompany.com:7499,idmhost2.mycompany.com:7499
</Location>
```

After editing, the file should look like this:

```
<VirtualHost *:7777>
  ServerName https://sso.mycompany.com:443
  RewriteEngine On
  RewriteOptions inherit
  UseCanonicalName On
  -- added lines --
</VirtualHost>
```

Restart the Oracle HTTP Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

15.11 Validating Oracle Identity Federation

If the configuration is correct, you can access the following URL from a web browser:

`https://sso.mycompany.com/fed/sp/metadata`

You should see metadata.

15.12 Backing Up the Application Tier Configuration

It is an Oracle best practices recommendation to create a backup after successfully completing the installation and configuration of each tier, or at another logical point. Create a backup after verifying that the installation so far is successful. This is a quick backup for the express purpose of immediate restoration in case of problems in later steps. The backup destination is the local disk. You can discard this backup when the enterprise deployment setup is complete. After the enterprise deployment setup is complete, you can initiate the regular deployment-specific Backup and Recovery process. For more details, see the *Oracle Fusion Middleware Administrator's Guide*.

For information on database backups, refer to the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation to this point, follow these steps:

1. Back up the web tier as described in [Section 7.6, "Backing up the Web Tier Configuration."](#)
2. Back up the database. This is a full database backup, either hot or cold. The recommended tool is Oracle Recovery Manager.

3. Back up the application tier instances by following these steps:
 - a. Shut down the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```
 - b. Create a backup of the Middleware home on the application tier. On Linux, as the `root` user, type:

```
tar -cvpf BACKUP_LOCATION/apptier.tar MW_HOME
```
 - c. Create a backup of the Instance home on the application tier as the `root` user:

```
tar -cvpf BACKUP_LOCATION/instance_backup.tar ORACLE_INSTANCE
```
 - d. Start up the instance using `opmnctl` located under the `ORACLE_INSTANCE/bin` directory:

```
ORACLE_INSTANCE/bin/opmnctl startall
```
4. Back up the Administration Server domain directory as described in [Section 8.10, "Backing Up the WebLogic Domain."](#)
5. Back up the Oracle Internet Directory as described in [Section 9.8, "Backing up the Oracle Internet Directory Configuration."](#)
6. Back up the Oracle Virtual Directory as described in [Section 12.9, "Backing Up the Oracle Virtual Directory Configuration."](#)

Setting Up Node Manager for an Enterprise Deployment

This chapter describes how to configure Node Manager in accordance with Oracle best practice recommendations.

This chapter contains the following sections:

- [Section 16.1, "Overview of the Node Manager"](#)
- [Section 16.2, "Changing the Location of the Node Manager Log"](#)
- [Section 16.3, "Enabling Host Name Verification Certificates for Node Manager"](#)
- [Section 16.4, "Starting Node Manager"](#)

16.1 Overview of the Node Manager

Node Manager enables you to start and stop the Administration Server and the Managed Servers.

Process

The procedures described in this chapter must be performed for various components of the enterprise deployment topologies outlined in [Section 2.1.1, "Reference Topologies Documented in the Guide."](#) The topologies and hosts are shown in [Table 16–1](#).

Table 16–1 *Hosts in Each Topology*

Topology	Hosts
OAM11g	IDMHOST1
	IDMHOST2
OAM11g/OIM11g	IDMHOST1
	IDMHOST2
	OIMHOST1
	OIMHOST2
OIF11g	IDMHOST1
	IDMHOST2

Note that the procedures in this chapter must be performed multiple times for each VIP-and-IP pair using the information provided in the component-specific chapters.

Recommendations

Oracle provides two main recommendations for Node Manager configuration in enterprise deployment topologies:

1. Oracle recommends placing the Node Manager log file in a location different from the default one (which is inside the Middleware Home where Node Manager resides). See [Section 16.2, "Changing the Location of the Node Manager Log"](#) for further details.
2. Oracle also recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses used in the domain. This chapter explains the steps for configuring certificates in the hosts for host name verification. See [Section 16.3, "Enabling Host Name Verification Certificates for Node Manager"](#) for further details.

Note: The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that consist of random sequences of both uppercase and lowercase characters as well as numbers.

16.2 Changing the Location of the Node Manager Log

Edit the Node Manager properties file located at `MW_HOME/wlserver_10.3/common/nodemanager/nodemanager.properties`. Add the new location for the log file using the following line:

```
LogFile=ORACLE_BASE/admin/nodemanager.log
```

Oracle best practice is to use a location outside the `MW_HOME` directory and inside the administration directory.

Restart Node Manager, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) for the change to take effect.

16.3 Enabling Host Name Verification Certificates for Node Manager

This section describes how to set up host name verification certificates for communication between Node Manager and the Administration Server. It consists of the following steps:

- [Section 16.3.1, "Generating Self-Signed Certificates Using the utils.CertGen Utility"](#)
- [Section 16.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility"](#)
- [Section 16.3.3, "Creating a Trust Keystore Using the Keytool Utility"](#)
- [Section 16.3.4, "Configuring Node Manager to Use the Custom Keystores"](#)
- [Section 16.3.5, "Using a Common or Shared Storage Installation"](#)
- [Section 16.3.6, "Configuring Managed WebLogic Servers to Use the Custom Keystores"](#)
- [Section 16.3.7, "Changing the Host Name Verification Setting for the Managed Servers"](#)

16.3.1 Generating Self-Signed Certificates Using the `utils.CertGen` Utility

The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (*HOST.mycompany.com*) and a WebLogic Managed Server listens on a virtual host name (*VIP.mycompany.com*). Whenever a server is using a virtual host name, it is implied that the server can be migrated from one node to another. Consequently, the directory where keystores and trust keystores are maintained ideally must reside on a shared storage that is accessible from the failover. If additional host names are used in the same or different nodes, the steps in this example must be extended to:

1. Add the required host names to the certificate stores (if they are different from *HOST.mycompany.com* and *VIP.mycompany.com*).
2. Change the identity and trust store location information for Node Manager (if the additional host names are used by Node Manager) or for the servers (if the additional host names are used by Managed Servers).

Follow these steps to create self-signed certificates on *HOST*. These certificates should be created using the network name or alias. For information on using trust CA certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*. The following examples configure certificates for *HOST.mycompany.com* and *VIP.mycompany.com*; that is, it is assumed that both a physical host name (*HOST*) and a virtual host name (*VIP*) are used in *HOST*. It is also assumed that *HOST.mycompany.com* is the address used by Node Manager and *VIP.mycompany.com* is the address used by a Managed Server or the Administration Server. This is the common situation for nodes hosting an Administration Server and a Fusion Middleware component, or for nodes where two Managed Servers coexist with one server listening on the physical host name and one server using a virtual host name (which is the case for servers that use migration servers).

1. Set up your environment by running the `WL_HOME/server/bin/setWLSEnv.sh` script. In the Bourne shell, run the following commands:

```
cd WL_HOME/server/bin
. ./setWLSEnv.sh
```

Verify that the `CLASSPATH` environment variable is set:

```
echo $CLASSPATH
```

2. Create a user-defined directory for the certificates. For example, create a directory called 'certs' under the `ORACLE_BASE/admin/domain_name/aserver/domain_name` directory. Note that certificates can be shared across WebLogic domains.

```
cd ORACLE_BASE/admin/domain_name/aserver/domain_name
mkdir certs
```

Note: The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (like SSL set up for HTTP invocations, for example).

3. Change directory to the directory that you just created:

```
cd certs
```

4. Run the `utils.CertGen` tool from the user-defined directory to create the certificates for both *HOST*. `mycompany.com` and *VIP*. `mycompany.com`.

Syntax (all on a single line):

```
java utils.CertGen Key_Passphrase Cert_File_Name Key_File_Name  
[export | domestic] [Host_Name]
```

Examples:

```
java utils.CertGen Key_Passphrase IDMHOST1.mycompany.com_cert  
IDMHOST1.mycompany.com_key domestic IDMHOST1.mycompany.com
```

```
java utils.CertGen Key_Passphrase IDMHOST2.mycompany.com_cert  
IDMHOST2.mycompany.com_key domestic IDMHOST2.mycompany.com
```

```
java utils.CertGen Key_Passphrase ADMINVHN.mycompany.com_cert  
ADMINVHN.mycompany.com_key domestic ADMINVHN.mycompany.com
```

```
java utils.CertGen Key_Passphrase OIMADMINVHN.mycompany.com_cert  
OIMADMVHN.mycompany.com_key domestic OIMADMINVHN.mycompany.com
```

Also create a certificate for the Admin Server virtual host.

```
java utils.CertGen Key_Passphrase OIMADMINVHN.mycompany.com_cert  
OIMADMINVHN.mycompany.com_key domestic OIMADMINVHN.mycompany.com
```

16.3.2 Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility

Follow these steps to create an identity keystore on `IDMHOST1`:

1. Create a new identity keystore called `appIdentityKeyStore` using the `utils.ImportPrivateKey` utility. Create this keystore under the same directory as the certificates (that is, `ORACLE_BASE/admin/domain_name/aserver/domain_name/certs`).

Note: The Identity Store is created (if none exists) when you import a certificate and the corresponding key into the Identity Store using the `utils.ImportPrivateKey` utility.

2. Import the certificate and private key for `IDMHOST1.mycompany.com`, `IDMHOST2.mycompany.com` and `ADMINVHN.mycompany.com` or `OIMADMVHN.mycompany.com` into the Identity Store. Ensure that you use a different alias for each of the certificate/key pairs imported.

Syntax (all on a single line):

```
java utils.ImportPrivateKey Keystore_File Keystore_Password  
Certificate_Alias_to_Use Private_Key_Passphrase  
Certificate_File  
Private_Key_File  
[Keystore_Type]
```

Examples:

```
java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase  
appIdentityIDMHOST1 Key_Passphrase ASERVER_HOME/certs/IDMHOST1.mycompany.com_
```



```

cert.pem ASERVER_HOME/certs/IDMHOST1.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityIDMHOST2 Key_Passphrase ASERVER_HOME/certs/IDMHOST2.mycompany.com_
cert.pem ASERVER_HOME/certs/IDMHOST2.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityADMVHN Key_Passphrase ASERVER_HOME/certs/ADMINVNH.mycompany.com_
cert.pem ASERVER_HOME/certs/ADMINVNH.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityOIMADMVHN Key_Passphrase ASERVER_HOME/certs/OIMADMVHN.mycompany.com_
cert.pem ASERVER_HOME/certs/OIMADMVHN.mycompany.com_key.pem

java utils.ImportPrivateKey appIdentityKeyStore.jks Key_Passphrase
appIdentityADMVHN Key_Passphrase ASERVER_HOME/certs/OIMADMVHN.mycompany.com_
cert.pem ASERVER_HOME/certs/OIMADMVHN.mycompany.com_key.pem

```

16.3.3 Creating a Trust Keystore Using the Keytool Utility

Follow these steps to create the trust keystore on each host, for example IDMHOST1 and IDMHOST2:

1. Copy the standard Java keystore to create the new trust keystore since it already contains most of the root CA certificates needed. Oracle does not recommend modifying the standard Java trust keystore directly. Copy the standard Java keystore CA certificates located under the `WL_HOME/server/lib` directory to the same directory as the certificates. For example:

```
cp WL_HOME/server/lib/cacerts ASERVER_HOME/certs/appTrustKeyStoreIDMHOST1.jks
```

2. The default password for the standard Java keystore is `changeit`. Oracle recommends always changing the default password. Use the `keytool` utility to do this. The syntax is:

```
keytool -storepasswd -new New_Password -keystore Trust_Keystore -storepass
Original_Password
```

For example:

```
keytool -storepasswd -new Key_Passphrase -keystore appTrustKeyStoreIDMHOST1.jks
-storepass changeit
```

3. The CA certificate `CertGenCA.der` is used to sign all certificates generated by the `utils.CertGen` tool. It is located in the `WL_HOME/server/lib` directory. This CA certificate must be imported into the `appTrustKeyStore` using the `keytool` utility. The syntax is:

```
keytool -import -v -noprompt -trustcacerts -alias Alias_Name
-file CA_File_Location -keystore Keystore_Location -storepass Keystore_Password
```

For example:

```
keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_
HOME/server/lib/CertGenCA.der -keystore appTrustKeyStoreIDMHOST1.jks -storepass
Key_Passphrase
```

16.3.4 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores, add the following lines to the end of the `nodemanager.properties` file located in the `WL_HOME/common/nodemanager` directory:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

For example:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=ORACLE_BASE/admin/domain_name/aserver/domain_
name/certs/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=Key_Passphrase
CustomIdentityAlias=appIdentityIDMHOST1
CustomIdentityPrivateKeyPassPhrase=Key_Passphrase
```

The passphrase entries in the `nodemanager.properties` file get encrypted when you start Node Manager as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#) For security reasons, minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, start Node Manager as soon as possible so that the entries get encrypted.

16.3.5 Using a Common or Shared Storage Installation

When using a common or shared storage installation for `MW_HOME`, Node Manager is started from different nodes using the same base configuration (`nodemanager.properties`). Add the certificate for all the nodes that share the binaries to the `appIdentityKeyStore.jks` identity store by creating the certificate for the new node and import it to `appIdentityKeyStore.jks`, as described in [Section 16.3.1, "Generating Self-Signed Certificates Using the `utils.CertGen` Utility."](#) Once the certificates are available in the store, each node manager must point to a different identity alias to send the correct certificate to the Administration Server.

To set different environment variables before starting Node Manager in the different nodes:

```
cd WL_HOME/server/bin
export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityIDMHOST1

cd WL_HOME/server/bin
export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityIDMHOST2
```

Note: Make sure to specify the custom identity alias specifically assigned to each host, for example `appIdentity1` for `...HOST1` and `appIdentity2` for `...HOST2`.

16.3.6 Configuring Managed WebLogic Servers to Use the Custom Keystores

Follow these steps to configure the identity and trust keystores for `WLS_SERVER`:

1. Log in to Oracle WebLogic Server Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click **Lock and Edit**.

3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Click the name of the server for which you want to configure the identity and trust keystores (*WLS_SERVER*). The settings page for the selected server is displayed.
6. Select **Configuration**, then **Keystores**.
7. In the Keystores field, select the **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA certificates.
8. In the Identity section, define attributes for the identity keystore:
 - **Custom Identity Keystore:** The fully qualified path to the identity keystore:
`ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/appIdentityKeyStore.jks`
 - **Custom Identity Keystore Type:** Leave blank; it defaults to JKS.
 - **Custom Identity Keystore Passphrase:** The password (*Keystore_Password*) you provided in [Section 16.3.3, "Creating a Trust Keystore Using the Keytool Utility."](#) This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.
9. In the Trust section, define properties for the trust keystore:
 - **Custom Trust Keystore:** The fully qualified path to the trust keystore:
`ORACLE_BASE/admin/domain_name/aserver/domain_name/certs/appTrustKeyStoreIDMHOST1.jks`
 - **Custom Trust Keystore Type:** Leave blank; it defaults to JKS.
 - **Custom Trust Keystore Passphrase:** The password you provided as *New_Password* in [Section 16.3.3, "Creating a Trust Keystore Using the Keytool Utility."](#) This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server only reads from the keystore, so whether you define this property depends on the requirements of the keystore.
10. Click **Save**.
11. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
12. Select **Configuration**, then **SSL**.
13. Click **Lock and Edit**.
14. In the **Private Key Alias** field, enter the alias you used for the host name the Managed Server listens on, for example:
 - For *wls_ods1*, use *appIdentityIDMHOST1*.
 - For *wls_ods2* use *appIdentityIDMHOST2*.
 - For *ADMINSERVER* user *appIdentityADMVHN*.

In the **Private Key Passphrase** and the **Confirm Private Key Passphrase** fields, enter the password for the keystore that you created in [Section 16.3.2, "Creating an Identity Keystore Using the `utils.ImportPrivateKey` Utility."](#)

15. Click **Save**.
16. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
17. Restart the server for which the changes have been applied, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

16.3.7 Changing the Host Name Verification Setting for the Managed Servers

Once the previous steps have been performed, set host name verification for the affected Managed Servers to `Bea Hostname Verifier`. To do this, perform the following steps:

1. Log in to Oracle WebLogic Server Administration Console.
2. Select **Lock and Edit** from the change center.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select the Managed Server in the Names column of the table. The settings page for the server is displayed.
6. Open the SSL tab.
7. Expand the **Advanced** section of the page.
8. Set host name verification to `Bea Hostname Verifier`.
9. Click **Save**.
10. Click **Activate Changes**.

16.4 Starting Node Manager

Run the following commands to start Node Manager.

Note: If you have not configured and started Node Manager for the first time yet, run the `setNMProps.sh` script as specified in [Section 8.7.3, "Starting Node Manager."](#) This enables the use of the start script that is required for Identity Management Components.

```
cd WL_HOME/server/bin
./startNodeManager.sh
```

Note: Verify that Node Manager is using the appropriate stores and alias from the Node Manager output. You should see the following when Node Manager starts.:

```
<Loading identity key store:  
  FileName=ASERVER_HOME/certs/appIdentityKeyStore.jks, Type=jks,  
  PassPhraseUsed=true>
```

Host name verification works if you apply a test configuration change to the servers and it succeeds without Node Manager reporting any SSL errors.

Configuring Server Migration for an Enterprise Deployment

Configuring server migration allows SOA- and OIM-managed servers to be migrated from one host to another, so that if a node hosting one of the servers fails, the service can continue on another node. This chapter describes how to configure server migration for an Identity Management enterprise deployment.

This chapter contains the following steps:

- [Section 17.1, "Overview of Server Migration for an Enterprise Deployment"](#)
- [Section 17.2, "Setting Up a User and Tablespace for the Server Migration Leasing Table"](#)
- [Section 17.3, "Creating a Multi Data Source Using the Oracle WebLogic Administration Console"](#)
- [Section 17.4, "Editing Node Manager's Properties File"](#)
- [Section 17.5, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"](#)
- [Section 17.6, "Configuring Server Migration Targets"](#)
- [Section 17.7, "Testing the Server Migration"](#)

17.1 Overview of Server Migration for an Enterprise Deployment

Configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers. The WLS_OIM1 and WLS_SOA1 Managed Server are configured to restart on OIMHOST2 should a failure occur. The WLS_OIM2 and WLS_SOA2 Managed Servers are configured to restart on OIMHOST1 should a failure occur. The WLS_OIM1, WLS_SOA1, WLS_OIM2 and WLS_SOA2 servers listen on specific floating IPs that are failed over by WebLogic Server Migration.

Perform the steps in the following sections configure server migration for the WLS_OIM1, WLS_SOA1, WLS_OIM2, and WLS_SOA2 Managed Servers.

17.2 Setting Up a User and Tablespace for the Server Migration Leasing Table

In this section, you set up a user and tablespace for the server migration leasing table:

Note: If other servers in the same domain have already been configured with server migration, the same tablespace and data sources can be used. In that case, the data sources and multi data source for database leasing do not need to be re-created, but they must be retargeted to the clusters being configured with server migration.

1. Create a tablespace called `leasing`. For example, log on to SQL*Plus as the `sysdba` user and run the following command:

```
create tablespace leasing
logging datafile 'DB_HOME/oradata/orcl/leasing.dbf'
size 32m autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named `leasing` and assign to it the `leasing` tablespace:

```
create user leasing identified by welcome1;
grant create table to leasing;
grant create session to leasing;
alter user leasing default tablespace leasing;
alter user leasing quota unlimited on LEASING;
```

3. Create the `leasing` table using the `leasing.ddl` script:

- a. Copy the `leasing.ddl` file located in either of the following directories to your database node:

```
WL_HOME/server/db/oracle/817
WL_HOME/server/db/oracle/920
```

- b. Connect to the database as the `leasing` user.
- c. Run the `leasing.ddl` script in SQL*Plus:

```
@Copy_Location/leasing.ddl;
```

17.3 Creating a Multi Data Source Using the Oracle WebLogic Administration Console

The second step is to create a multi data source for the `leasing` table from the Oracle WebLogic Server Administration Console. You create a data source to each of the Oracle RAC database instances during the process of setting up the multi data source, both for these data sources and the global leasing multi data source. When you create a data source:

- Ensure that this is a non-XA data source.
- The names of the multi data sources are in the format of *MultiDS-rac0*, *MultiDS-rac1*, and so on.
- Use Oracle's Driver (Thin) Version 9.0.1, 9.2.0, 10, 11.
- Data sources do not require support for global transactions. Therefore, do *not* use any type of distributed transaction emulation/participation algorithm for the data source (do not choose the **Supports Global Transactions** option, or the **Logging Last Resource, Emulate Two-Phase Commit**, or **One-Phase Commit** options of the **Supports Global Transactions** option), and specify a service name for your database.
- Target these data sources to the `oim_cluster` and the `soa_cluster`.

- Ensure the data source's connection pool initial capacity is set to 0 (zero). To do this, select **Services**, **JDBC**, and then **Datasources**. In the Datasources screen, click the **Datasource Name**, then click the **Connection Pool** tab, and enter 0 (zero) in the **Initial Capacity** field.

Creating a Multi Data Source

Perform these steps to create a multi data source:

1. From Domain Structure window in the Oracle WebLogic Server Administration Console, expand the **Services** node. The Summary of JDBC Data Source page appears.
2. Click **Data Sources**. The Summary of JDBC Multi Data Source page is displayed.
3. Click **Lock and Edit**.
4. Click **New Multi Data Source**. The Create a New JDBC Multi Data Source page is displayed.
5. Enter `leasing` as the name.
6. Enter `jdbc/leasing` as the JNDI name.
7. Select **Failover** as algorithm (default).
8. Click **Next**.
9. Select **oim_cluster** and **soa_cluster** as the targets.
10. Click **Next**.
11. Select **non-XA driver** (the default).
12. Click **Next**.
13. Click **Create New Data Source**.
14. Enter `leasing-rac0` as the name. Enter `jdbc/leasing-rac0` as the JNDI name. Enter `oracle` as the database type. For the driver type, select Oracle Driver (Thin) for Oracle RAC Service-Instance connections, Versions:10 and later.

Note: When creating the multi data sources for the leasing table, enter names in the format of *MultiDS-rac0*, *MultiDS-rac1*, and so on.

15. Click **Next**.
16. On JDBC Data Source Properties, select **Database Driver: Oracle's Driver (Thin) for RAC Service-Instance connections**.
17. Deselect **Supports Global Transactions**.
18. Click **Next**.
19. Enter the service name, database name, host port, and password for your leasing schema.
20. Click **Next**.
21. Click **Test Configuration** and verify that the connection works.
22. Click **Next**.
23. Target the data source to **oim_cluster** and **SOA cluster**.

24. Click **Finish**.
25. Select the data source you just created, for example `leasing-rac0`, and add it to the right screen.
26. Click **Create a New Data Source** for the second instance of your Oracle RAC database, target it to the `oim_cluster` and `soa_cluster`, repeating the steps for the second instance of your Oracle RAC database.
27. Add the second data source to your multi data source.
28. Click **Activate Changes**.

17.4 Editing Node Manager's Properties File

In this section, you edit Node Manager's properties file. This must be done for the Node Managers on the nodes where the servers are running, OIMHOST1 and OIMHOST2.

The `nodemanager.properties` file is located in the following directory:

`WL_HOME/common/nodemanager`

Add the following properties to enable server migration to work properly:

- **Interface:**

`Interface=eth0`

This property specifies the interface name for the floating IP (for example, `eth0`).

Note: Do not specify the sub-interface, such as `eth0:1` or `eth0:2`. This interface is to be used without `:0` or `:1`. Node Manager's scripts traverse the different `:X`-enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, `eth2`, `eth3`, `ethn`, depending on the number of interfaces configured.

- **NetMask:**

`NetMask=255.255.255.0`

This property specifies the net mask for the interface for the floating IP. The net mask should be the same as the net mask on the interface.

- **UseMACBroadcast:**

`UseMACBroadcast=true`

This property specifies whether to use a node's MAC address when sending ARP packets, that is, whether to use the `-b` flag in the `arping` command.

Verify in Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
StateCheckInterval=500
eth0=*,NetMask=255.255.248.0
UseMACBroadcast=true
```

Note: The following steps are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

1. If not done already, set the `StartScriptEnabled` property in the `nodemanager.properties` file to `true`. This is required to enable Node Manager to start the managed servers.
2. Start Node Manager on `OIMHOST1` and `OIMHOST2` by running the `startNodeManager.sh` script, which is located in the `WL_HOME/server/bin` directory.

Note: When running Node Manager from a shared storage installation, multiple nodes are started using the same `nodemanager.properties` file. However, each node may require different `NetMask` or `Interface` properties. In this case, specify individual parameters on a per-node basis using environment variables. For example, to use a different interface (`eth3`) in `HOSTn`, use the `Interface` environment variable as follows:

```
export JAVA_OPTIONS=-DInterface=eth3
```

and start Node Manager after the variable has been set in the shell.

17.5 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

This section is not required on Windows. On Linux, you set environment and superuser privileges for the `wlsifconfig.sh` script:

Ensure that your `PATH` environment variable includes the files listed in [Table 17-1](#).

Table 17-1 Files Required for the PATH Environment Variable

File	Located in this directory
<code>wlsifconfig.sh</code>	<code>ORACLE_BASE/admin/domain_name/msserver/domain_name/bin/server_migration</code>
<code>wlscontrol.sh</code>	<code>WL_HOME/common/bin</code>
<code>nodemanager.domains</code>	<code>WL_HOME/common/nodemanager</code>

Grant `sudo` privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries.

For security reasons, `sudo` should be restricted to the subset of commands required to run the `wlsifconfig.sh` script. For example, perform the following steps to set the environment and superuser privileges for the `wlsifconfig.sh` script.

Note: Ask the system administrator for the appropriate `sudo` and system rights to perform this step.

Grant `sudo` privilege to the WebLogic user `oracle` with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries.

Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside */etc/sudoers* granting sudo execution privilege for `oracle` and also over `ifconfig` and `arping`.

To grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the */sbin/ifconfig* and */sbin/arping* binaries:

```
Defaults:oracle !requiretty
oracle ALL=NOPASSWD: /sbin/ifconfig, /sbin/arping
```

17.6 Configuring Server Migration Targets

In this section, you configure server migration targets. Configuring Cluster Migration sets the `DataSourceForAutomaticMigration` property to `true`.

To configure migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration (**oim_cluster**) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock and Edit**.
6. In the **Available** field, select the machine to which to allow migration and click the right arrow. In this case, select **OIMHOST1** and **OIMHOST2**.
7. Select the data source to be used for automatic migration. In this case, select the leasing data source.
8. Click **Save**.
9. Click **Activate Changes**.
10. Repeat steps 2 through 9 for the SOA cluster.
11. Set the candidate machines for server migration. You must perform this task for all of the Managed Servers as follows:
 - a. Click **Lock and Edit**.
 - b. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.
 - c. Select the server for which you want to configure migration.
 - d. Click the **Migration** tab.
 - e. In the **Available** field, located in the Migration Configuration section, select the machines to which to allow migration and click the right arrow. For **WLS_OIM1**, select **OIMHOST2**. For **WLS_OIM2**, select **OIMHOST1**.
 - f. Select **Automatic Server Migration Enabled** and click **Save**.

This enables Node Manager to start a failed server on the target node automatically.
 - g. Click **Activate Changes**.

- h. Repeat the previous steps for the WLS_SOA1 and WLS_SOA2 Managed Servers.
- i. Restart WebLogic Administration Server, Node Managers, and the servers for which server migration has been configured, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

Tip: Click **Customize this table** in the Summary of Servers page and move Current Machine from the Available window to the Chosen window to view the machine on which the server is running. This is different from the configuration if the server is migrated automatically.

17.7 Testing the Server Migration

In this section, you test the server migration. Perform these steps to verify that server migration is working properly:

To test from OIMHOST1:

1. Stop the WLS_OIM1 Managed Server. To do this, run this command:

```
kill -9 pid
```

where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

```
ps -ef | grep WLS_OIM1
```

2. Watch the Node Manager console. You should see a message indicating that WLS_OIM1's floating IP has been disabled.
3. Wait for Node Manager to try a second restart of WLS_OIM1. It waits for a fence period of 30 seconds before trying this restart.
4. Once Node Manager restarts the server, stop it again. Node Manager should now log a message indicating that the server will not be restarted again locally.

To test from OIMHOST2:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart WLS_OIM1 on OIMHOST1, Node Manager on OIMHOST2 should prompt that the floating IP for WLS_OIM1 is being brought up and that the server is being restarted in this node.
2. Access the OIM Console using the Virtual Host Name, for example: OIMVH1.

Follow the previous steps to test server migration for the WLS_OIM2, WLS_SOA1, and WLS_SOA2 Managed Servers.

[Table 17-2](#) shows the Managed Servers and the hosts they migrate to in case of a failure.

Table 17-2 WLS_OIM1, WLS_OIM2, WLS_SOA1, WLS_SOA2 Server Migration

Managed Server	Migrated From	Migrated To
WLS_OIM1	OIMHOST1	OIMHOST2
WLS_OIM2	OIMHOST2	OIMHOST1
WLS_SOA1	OIMHOST1	OIMHOST2
WLS_SOA2	OIMHOST2	OIMHOST1

Verification From the Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the Administration Console.
2. Click **Domain** on the left console.
3. Click the **Monitoring** tab and then the **Migration** sub tab.

The Migration Status table provides information on the status of the migration.

Note: After a server is migrated, to fail it back to its original node/machine, stop the Managed Server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager starts the Managed Server on the machine to which it was originally assigned.

Integrating Oracle Identity Management Components for an Enterprise Deployment

This chapter describes how to integrate Oracle Identity Management components for an enterprise deployment.

This chapter contains the following sections:

- [Section 18.1, "Overview of Integrating Oracle Identity Management Components"](#)
- [Section 18.2, "Integrating Oracle Identity Manager and Oracle Access Manager 11g"](#)
- [Section 18.3, "Preparing the Environment for Fusion Applications Provisioning"](#)
- [Section 18.4, "Integrating Oracle Identity Federation with Oracle Access Manager 11g"](#)
- [Section 18.5, "Backing Up the Identity Management Configuration"](#)

18.1 Overview of Integrating Oracle Identity Management Components

Now that you have finished setting up the Identity Management environment, you must perform some final tasks to ensure that the components work together.

You must also ensure that the environment is ready for Fusion Applications provisioning.

18.2 Integrating Oracle Identity Manager and Oracle Access Manager 11g

This section describes how to integrate Oracle Identity Manager and Oracle Access Manager.

This section contains the following topics:

- [Section 18.2.1, "Prerequisites"](#)
- [Section 18.2.2, "Copying OAM Keystore Files to OIMHOST1 and OIMHOST2"](#)
- [Section 18.2.3, "About the Split Oracle Identity Manager Domain"](#)
- [Section 18.2.4, "Updating Existing LDAP Users with Required Object Classes"](#)
- [Section 18.2.5, "Integrating Oracle Access Manager 11g with Oracle Identity Manager 11g"](#)
- [Section 18.2.6, "Managing the Password of the xelsysadm User"](#)
- [Section 18.2.7, "Validating Integration."](#)

18.2.1 Prerequisites

1. Ensure that Oracle Identity Manager 11g has been installed and configured as described in [Chapter 14, "Configuring Oracle Identity Manager."](#)
2. Ensure that Oracle Access Manager 11g has been installed and configured as described in [Chapter 13, "Configuring Oracle Access Manager 11g."](#)
3. Ensure that OHS has been installed and configured as described in [Chapter 6.2, "Installing Oracle HTTP Server."](#)

18.2.2 Copying OAM Keystore Files to OIMHOST1 and OIMHOST2

If you are using Oracle Access Manager with the Simple Security Transport model, you must copy the OAM keystore files that were generated in [Section 13.10, "Creating Oracle Access Manager Key Store"](#) to OIMHOST1 and OIMHOST2. Copy the keystore files `ssoKeystore.jks` and `oamclient-truststore.jks` to the directory `MSERVER_HOME/domain_name/config/fmwconfig` on OIMHOST1 and OIMHOST2.

18.2.3 About the Split Oracle Identity Manager Domain

The examples in this chapter show integrating Oracle Identity Manager with other components in the domain IDMDomain to include Oracle Identity Manager. If you are building a split domain topology, substitute OIMDomain wherever you see a reference to IDMDomain and OIMADMINVHN wherever you see ADMINVHN.

18.2.4 Updating Existing LDAP Users with Required Object Classes

You must update existing LDAP users with the object classes `OblixPersonPwdPolicy`, `OIMPersonPwdPolicy`, and `OblixOrgPerson`.

Note: This is not required in the case of a fresh setup where you do not have any existing users.

On IDMHOST1, create a properties file for the integration called `user.props`, with the following contents:

```
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_PORT: 389
IDSTORE_ADMIN_USER: cn=orcladmin
IDSTORE_DIRECTORYTYPE: OVD
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
PASSWORD_EXPIRY_PERIOD: 7300
IDSTORE_LOGINATTRIBUTE: uid
```

Where:

- IDSTORE_HOST is the name of LDAP server. For example:
`idstore.mycompany.com`
- IDSTORE_PORT is the port of the LDAP server.
- IDSTORE_ADMIN_USER is the bind DN of an administrative user. For example:
`cn=orcladmin` or `cn=oudadmin`

- IDSTORE_DIRECTORYTYPE is the type of directory, valid values are OID and OVD.
- IDSTORE_USERSEARCHBASE is the location of users in the directory. For example:
cn=Users , dc=mycompany , dc=com
- IDSTORE_GROUPSEARCHBASE is the location of groups in the directory. For example:
cn=Groups , dc=mycompany , dc=com
- IDSTORE_LOGINATTRIBUTE this is the directory login attribute name. For example:
uid.
- PASSWORD_EXPIRY_PERIOD is the password expiry period.

Set the environment variables: MW_HOME, JAVA_HOME, IDM_HOME, and ORACLE_HOME.

Set IDM_HOME to *IDM_ORACLE_HOME*

Set ORACLE_HOME to *IAM_ORACLE_HOME*

Set MW_HOME to *MW_HOME*.

Set JAVA_HOME to *MW_HOME/jrockit-version*.

Upgrade existing LDAP, using the command `idmConfigTool`, which is located at:
IAM_ORACLE_HOME/idmtools/bin

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

IAM_ORACLE_HOME/idmtools/bin

The syntax of the command is:

```
idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=configfile
```

on Linux and

```
idmConfigTool.bat -upgradeLDAPUsersForSSO input_file=configfile
```

on Windows.

For example:

```
idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=user.props
```

When prompted, enter the password of the user you are using to connect to your Identity Store.

Sample output:

```
Enter LDAP admin user password:
```

```
***** Upgrading LDAP Users With OAM ObjectClasses *****
```

```
Completed loading user inputs for - LDAP connection info

Completed loading user inputs for - LDAP Upgrade

Upgrading ldap users at - cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=readOnlyUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=readWriteUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in
cn=oamMasterAdminUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
```

```
cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=oamSoftwareUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=PolStoreROUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in
cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in
cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in
cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=PolStoreRWUser,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=PUBLIC, cn=Users, dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in cn=PUBLIC, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixOrgPerson not present in cn=PUBLIC, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

objectclass OblixPersonPwdPolicy not present in cn=PUBLIC, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=PUBLIC, cn=Users, dc=us,dc=oracle,dc=com

Parsing - cn=orcladmin, cn=Users, dc=us,dc=oracle,dc=com

objectclass OIMPersonPwdPolicy not present in cn=orcladmin, cn=Users,
dc=us,dc=oracle,dc=com. Seeding it

obpasswordexpirydate added in cn=orcladmin, cn=Users, dc=us,dc=oracle,dc=com

Parsing - cn=xelsysadm,cn=Users,dc=us,dc=oracle,dc=com

Parsing - cn=xelsysadmin,cn=Users,dc=us,dc=oracle,dc=com
```

Finished parsing LDAP

LDAP Users Upgraded.

See Also: *Oracle Fusion Middleware Integration Overview for Oracle Identity Management Suite* for more information about the `idmConfigTool` command.

18.2.5 Integrating Oracle Access Manager 11g with Oracle Identity Manager 11g

Integrating Oracle Identity Manager with Oracle Access Manager using a WebGate profile employs an Oracle Access Manager Trusted Authentication Protocol (TAP) scheme. This is different from previous releases which used Network Assertion Protocol (NAP).

To integrate Oracle Access Manager 11g with Oracle Identity Manager, perform the following steps on IDMHOST1 or OIMHOST1:

1. Set the Environment Variables `IDM_HOME` and `ORACLE_HOME`, for example:

```
export IDM_HOME=IDM_ORACLE_HOME
export ORACLE_HOME=IAM_ORACLE_HOME
```

2. Create a properties file for the integration called `oim1tg.props`, with the following contents.

Single Domain

Use the following contents if all your components are in a single domain:

```
LOGINURI: /${app.context}/adfAuthentication
LOGOUTURI: /oamsso/logout.html
AUTOLOGINURI: None
ACCESS_SERVER_HOST: IDMHOST1.mycompany.com
ACCESS_SERVER_PORT: 5575
ACCESS_GATE_ID: Webgate_IDM
COOKIE_DOMAIN: .mycompany.com
COOKIE_EXPIRY_INTERVAL: 120
OAM_TRANSFER_MODE: simple
WEBGATE_TYPE: ohsWebgate11g
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 389
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_DIRECTORYTYPE: OID or OVD
IDSTORE_ADMIN_USER: cn=oamLDAP,cn=Users,dc=mycompany,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
MDS_DB_URL: jdbc:oracle:thin:@(DESCRIPTION=(LOAD_
BALANCE=on)(FAILOVER=on)(ADDRESS_
LIST=(ADDRESS=(protocol=tcp)(host=OIDDBHOST1-vip.mycompany.com)(port=1521))(ADD
RESS=(protocol=tcp)(host=OIDDBHOST2-vip.mycompany.com)(port=1521)))(CONNECT_
DATA=(SERVER=DEDICATED)(SERVICE_NAME=oidedg.mycompany.com)))
MDS_DB_SCHEMA_USERNAME: edg_mds
WLSHOST: adminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
DOMAIN_NAME: IDMDomain
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain
```

IDSTORE_LOGINATTRIBUTE: uid

Split Domain

Use the following contents if your Oracle Identity Manager components are in a different domain from your Oracle Access Manager components:

```

LOGINURI: /${app.context}/adfAuthentication
LOGOUTURI: /oamsso/logout.html
AUTOLOGINURI: None
ACCESS_SERVER_HOST: IDMHOST1.mycompany.com
ACCESS_SERVER_PORT: 5575
ACCESS_GATE_ID: Webgate_IDM
COOKIE_DOMAIN: .mycompany.com
COOKIE_EXPIRY_INTERVAL: 120
IDSTORE_LOGINATTRIBUTE: uid
OAM_TRANSFER_MODE: simple
WEBGATE_TYPE: ohsWebgate11g
SSO_ENABLED_FLAG: true
IDSTORE_PORT: 389
IDSTORE_HOST: idstore.mycompany.com
IDSTORE_DIRECTORYTYPE: OID or OVD
IDSTORE_ADMIN_USER: cn=oamLDAP,cn=Users,dc=mycompany,dc=com
IDSTORE_USERSEARCHBASE: cn=Users,dc=mycompany,dc=com
IDSTORE_GROUPSEARCHBASE: cn=Groups,dc=mycompany,dc=com
MDS_DB_URL: jdbc:oracle:thin:@(DESCRIPTION=(LOAD_
BALANCE=on)(FAILOVER=on)(ADDRESS_
LIST=(ADDRESS=(protocol=tcp)(host=OIDDBHOST1-vip.mycompany.com)(port=1521))(ADD
RESS=(protocol=tcp)(host=OIDDBHOST2-vip.mycompany.com)(port=1521)))(CONNECT_
DATA=(SERVER=DEDICATED)(SERVICE_NAME=oidedg.mycompany.com)))
MDS_DB_SCHEMA_USERNAME: edg_mds
WLSHOST: oimadminvhn.mycompany.com
WLSPORT: 7001
WLSADMIN: weblogic
OAM11G_WLS_ADMIN_HOST: adminvhn.mycompany.com
OAM11G_WLS_ADMIN_PORT: 7001
OAM11G_WLS_ADMIN_USER: weblogic
DOMAIN_NAME: OIMDomain
OIM_MANAGED_SERVER_NAME: WLS_OIM1
DOMAIN_LOCATION: ORACLE_BASE/admin/OIMDomain/aserver/OIMDomain

```

Notes:

- Set `IDSTORE_HOST` to your Oracle Internet Directory host or load balancer name if you are using Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory host or load balancer name.
 - Set `IDSTORE_DIRECTORYTYPE` to `OVD` if you are using Oracle Virtual Directory server to connect to either a non-OID directory or Oracle Internet Directory. Set it to `OID` if your Identity Store is in Oracle Internet Directory and you are accessing it directly rather than through Oracle Virtual Directory.
 - If your access manager servers are configured to accept requests using the simple mode, set `OAM_TRANSFER_MODE` to `simple`. Otherwise set `OAM_TRANSFER_MODE` to `open`.
 - Set `IDSTORE_PORT` to your Oracle Internet Directory port if you are using Oracle Internet Directory as your Identity Store. If not, set it to your Oracle Virtual Directory port.
 - If you are using a single instance database, then set `MDS_URL` to:
`jdbc:oracle:thin:@DBHOST:1521:SID`
 - If your Oracle Identity Manager components are in a separate domain from your Oracle Access Manager components, you must specify the details of the OAM Domain using the parameters:
`OAM11G_WLS_ADMIN_HOST`, `OAM11G_WLS_ADMIN_PORT` and `OAM11G_WLS_ADMIN_USER`.
-

3. Integrate Oracle Access Manager with Oracle Identity Manager using the command `idmConfigTool`, which is located at:

`IAM_ORACLE_HOME/idmtools/bin`

Note: When you run the `idmConfigTool`, it creates or appends to the file `idmDomainConfig.param`. This file is generated in the same directory that the `idmConfigTool` is run from. To ensure that each time the tool is run, the same file is appended to, always run the `idmConfigTool` from the directory:

`IAM_ORACLE_HOME/idmtools/bin`

The syntax of the command is

```
idmConfigTool.sh -configOIM input_file=configfile
```

on Linux and

```
idmConfigTool.bat -configOIM input_file=configfile
```

on Windows.

For example:

```
IAM_ORACLE_HOME/idmtools/bin/idmConfigTool.sh -configOIM input_
file=oimtg.props
```

When the script runs you are prompted for the following information:

- Access Gate Password
- SSO Keystore Password
- Global Passphrase
- Idstore Admin Password
- MDS Database schema password
- Admin Server User Password

Sample output:

```
Enter sso access gate password :
Enter sso keystore jks password :
Enter sso global passphrase :
Enter mds db schema password :
Enter idstore admin password :
Enter admin server user password :
```

```
***** Seeding OAM Passwds in OIM *****
```

```
Completed loading user inputs for - CSF Config
```

```
Completed loading user inputs for - Dogwood Admin WLS
```

```
Connecting to t3://OAMADMINVHN.mycompany.com:7001
```

```
Connection to domain runtime mbean server established
```

```
Seeding credential :SSOAccessKey
```

```
Seeding credential :SSOGlobalPP
```

```
Seeding credential :SSOKeystoreKey
```

```
***** ***** *****
```

```
***** Activating OAM Notifications *****
```

```
Completed loading user inputs for - MDS DB Config
```

```
Apr 3, 2012 11:56:09 PM oracle.mds
```

```
NOTIFICATION: PManager instance is created without multitenancy support as JVM
flag "oracle.multitenant.enabled" is not set to enable multitenancy support.
Initialized MDS resources
```

```
Apr 3, 2012 11:56:09 PM oracle.mds
```

```
NOTIFICATION: PManager instance is created without multitenancy support as JVM
flag "oracle.multitenant.enabled" is not set to enable multitenancy support.
```

```
Apr 3, 2012 11:56:10 PM oracle.mds
```

```
NOTIFICATION: transfer operation started.
```

```
Apr 3, 2012 11:56:10 PM oracle.mds
```

```
NOTIFICATION: transfer is completed. Total number of documents successfully
processed : 1, total number of documents failed : 0.
```

```
Upload to DB completed
```

Releasing all resources

Notifications activated.

***** Seeding OAM Config in OIM *****

Completed loading user inputs for - OAM Access Config

Validated input values

Initialized MDS resources

Apr 3, 2012 11:56:10 PM oracle.mds

NOTIFICATION: PManager instance is created without multitenancy support as JVM flag "oracle.multitenant.enabled" is not set to enable multitenancy support.

Apr 3, 2012 11:56:10 PM oracle.mds

NOTIFICATION: transfer operation started.

Apr 3, 2012 11:56:10 PM oracle.mds

NOTIFICATION: transfer is completed. Total number of documents successfully processed : 1, total number of documents failed : 0.

Download from DB completed

Releasing all resources

Updated /u01/app/oracle/product/fmw/iam/server/oamMetadata/db/oim-config.xml

Initialized MDS resources

Apr 3, 2012 11:56:10 PM oracle.mds

NOTIFICATION: PManager instance is created without multitenancy support as JVM flag "oracle.multitenant.enabled" is not set to enable multitenancy support.

Apr 3, 2012 11:56:10 PM oracle.mds

NOTIFICATION: transfer operation started.

Apr 3, 2012 11:56:10 PM oracle.mds

NOTIFICATION: transfer is completed. Total number of documents successfully processed : 1, total number of documents failed : 0.

Upload to DB completed

Releasing all resources

OAM configuration seeded. Please restart oim server.

***** Configuring Authenticators in OIM WLS *****

Completed loading user inputs for - LDAP connection info

Connecting to t3://ADMINVHN.mycompany.com:7001


```
Connection to domain runtime mbean server established

Starting edit session

Edit session started

Connected to security realm.

Validating provider configuration

Validated desired authentication providers

Created OAMIDAsserter successfully

OAMIDAsserter is already configured to support 11g webgate

Created OIMSignatureAuthenticator successfully

Created OVDAuthenticator successfully

Setting attributes for OVDAuthenticator

All attributes set. Configured inOVDAuthenticatornow

LDAP details configured in OVDAuthenticator

Control flags for authenticators set sucessfully

Reordering of authenticators done sucessfully

Saving the transaction

Transaction saved

Activating the changes

Changes Activated. Edit session ended.

Connection closed sucessfully
```

```
*****
```

```
The tool has completed its operation. Details have been logged to
automation.log
```

Note: If you have already enabled single sign-on for your WebLogic Administration Consoles as described in [Section 19.3, "Create WebLogic Security Providers"](#) when this script is run, you might see the following errors when this script is run:

```
ERROR: Desired authenticators already present.
[Ljava.lang.String;@7fdb492]
ERROR: Error occurred while configuration. Authentication providers
to be configured already present.
ERROR: Rolling back the operation..
```

These errors can be ignored.

Note: You might see the following error messages:

```
SEVERE: Registering OIM as a TAP partner with OAM...
SEVERE: Registering OIM as a TAP partner with OAM was successful!!
SEVERE: Seeded OIM TAP partner key into Credential store
successfully...javax.crypto.spec.SecretKeySpec@fffe873d
SEVERE: Getting OAM/TAP Endpoint URL... SEVERE: Getting OAM/TAP
Endpoint URL was successful!!
```

These messages can be ignored.

4. Check the log file for errors and correct them if necessary.
5. Restart the Administration Servers as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#) If you are using a split domain, restart both servers.

18.2.6 Managing the Password of the xelsysadm User

After you integrate Oracle Identity Manager with Oracle Access Manager, two xelsysadm accounts exist. One is the internal account created by Oracle Identity Manager. The other is the account you created in the Identity Store in [Section 11.5, "Preparing the Identity Store."](#)

The xelsysadm account located in the LDAP store is the one used to access the OIM console. If you want to change the password of this account, change it in LDAP. You can use ODSM to do this. Do not change it through the OIM console.

18.2.7 Validating Integration

To validate integration, you must assign Identity Management administrators to WebLogic security groups and install WebGate as described in [Chapter 19, "Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment."](#)

To validate that the wiring of Oracle Access Manager 11g with Oracle Identity Manager 11g was successful, attempt to log in to the Oracle Identity Manager Self Service Console, as follows:

1. Using a browser, navigate to:
`https://sso.mycompany.com/oim`
This redirects you to the OAM11g single sign-on page.
2. Log in using the xelsysadm user account created in [Section 11.5, "Preparing the Identity Store."](#)
3. If you see the OIM Self Service Console Page, the integration was successful.

You can perform additional validation as follows:

1. Log in to the OIM Console as the xelsysadmn user.
2. Create a new user.
3. Log out as the xelsysadmn user.
4. Log in as the new user you just created. As the new user, you are redirected to the Password Management page.

5. Enter the credentials and click **Submit**. If integration has been performed correctly, you arrive at the page you are trying to access.

18.3 Preparing the Environment for Fusion Applications Provisioning

After the complete Identity Management environment is set up, prepare the environment for Fusion Applications provisioning, as described in this section.

This section contains the following topics:

- [Section 18.3.1, "About Input to the Fusion Applications Provisioning Tool"](#)
- [Section 18.3.2, "Creating a Client Keystore"](#)

18.3.1 About Input to the Fusion Applications Provisioning Tool

In earlier chapters, you were instructed to always run `idmConfigTool` from the same directory so that the tool would create or append to the file `idmDomainConfig.param.in` in that directory. The file `idmDomainConfig.param.in` in `IAM_ORACLE_HOME/idmtools/bin` now contains all the parameters that are required for Fusion Applications provisioning. Use that file as input to the Fusion Applications provisioning tool.

18.3.2 Creating a Client Keystore

To enable Fusion Applications to communicate with the Identity Management domain using SSL Server Authentication Mode, you must generate a client certificate and provide it to the Fusion Applications Provisioning process. You must provide a keystore containing the Trust point used by the Identity Management domain to the Fusion Applications.

Note:

If you are using Windows, you must install a UNIX emulation package such as Cygwin in order to run the scripts contained in this section. See <http://www.cygwin.com>.

When using Cygwin, ensure that you use the "/" character in path names when exporting a variable. For example:

```
export ORACLE_HOME=c:/oracle/idm
```

To generate a keystore containing a client certificate, perform the following steps:

1. Set the `ORACLE_HOME` and `JAVA_HOME` variables. For example, on LDAPHOST1, issue these commands:

```
export ORACLE_HOME=IDM_ORACLE_HOME
export PATH=$JAVA_HOME/bin:$PATH
```

2. To generate the certificate, use the tool `./SSLClientConfig.sh`, which is located in:

```
ORACLE_COMMON_HOME/bin
```

For example

```
./SSLClientConfig.sh -component cacert
```

As the command runs, enter the following values when prompted:

- LDAP Host Name: `policystore.mycompany.com`
- LDAP Port: `389`
- LDAP User: `cn=orcladmin`
- Password: *Password_for_cn=orcladmin*
- SSL Domain: `IDMDomain`
- Keystore Password: Enter a password to protect the keystore
- Confirm Password: Reenter the password.

The following is typical output from the command:

```
./SSLClientConfig.sh -component cacert
SSL Automation Script: Release 11.1.1.4.0 - Production
Copyright (c) 2010 Oracle. All rights reserved.
Downloading the CA certificate from a central LDAP location
Creating a common trust store in JKS and Oracle Wallet formats ...
Configuring SSL clients with the common trust store...
Make sure that your LDAP server is currently up and running.
Downloading the CA certificate from the LDAP server...
>>>Enter the LDAP hostname [LDAPHOST1.mycompany.com]: policystore.mycompany.com
>>>Enter the LDAP port: [3060]? 389
>>>Enter your LDAP user [cn=orcladmin]:
>>>Enter password for cn=orcladmin:
>>>Enter the sslDomain for the CA [idm]: IDMDomain
>>>Searching the LDAP for the CA usercertificate ...
Importing the CA certificate into trust stores...
>>>The common trust store in JKS format is located at
    /u01/app/oracle/product/fmw/IDM/rootCA/keystores/tmp/trust.jks
>>>The common trust store in Oracle wallet format is located at
    /u01/app/oracle/product/fmw/IDM/rootCA/keystores/tmp/ewallet.p12
Generate trust store for the CA cert at cn=IDMDomain,cn=sslDomains
>>>Enter a password to protect your truststore:
>>>Enter confirmed password for your truststore:

Create directory /u01/app/oracle/product/fmw/IDM/rootCA/keystores/common
Importing the CA certificate into trust stores...
>>>The common trust store in JKS format is located at
    /u01/app/oracle/product/fmw/IDM/rootCA/keystores/common/trust.jks
>>>The common trust store in Oracle wallet format is located at
    /u01/app/oracle/product/fmw/IDM/rootCA/keystores/common/ewallet.p12
```

This creates a file called `trust.jks` which must be provided to the Fusion Applications Provisioning process. After creating this certificate, you must delete the private key within this key. Use the following command:

```
keytool -delete -keystore trust.jks -alias testkey -storepass store_password
```

Oracle Fusion Applications provisioning uses this file to validate that the Identity Management installation is set up appropriately before provisioning takes place. In addition to this certificate, the keystore must also contain the certificate used by the load balancer for `sso.mycompany.com`.

Before you start this procedure, obtain a copy of the certificate by using your browser. First access `https://sso.mycompany.com:443`, then follow the instructions to download the certificate to a file. (Each browser does this differently.)

After you have obtained the certificate, load it into the keystore using the following command:

```
keytool -import -v -noprompt -trustcacerts -alias "OIM" -file loadbalancer.cer
-keystore trust.jks
```

where `loadbalancer.cer` is the name of the file where the load balancers SSL certificate is stored.

18.4 Integrating Oracle Identity Federation with Oracle Access Manager 11g

In Service Provider (SP) mode, Oracle Access Manager delegates user authentication to Oracle Identity Federation, which uses the Federation Oracle Single Sign-On protocol with a remote Identity Provider. Once the Federation Oracle Single Sign-On flow is performed, Oracle Identity Federation will create a local session and then propagates the authentication state to Oracle Access Manager, which maintains the session information.

This section provides the steps to integrate OIF with OAM11g in authentication mode and SP mode.

This section contains the following topics:

- [Section 18.4.1, "Prerequisites"](#)
- [Section 18.4.2, "Integrating Oracle Identity Federation with Oracle Access Manager in SP Mode"](#)

18.4.1 Prerequisites

Before starting this integration, ensure that the following tasks have been performed:

- Install and configure Oracle Identity Federation as described in [Chapter 15, "Extending the Domain to Include Oracle Identity Federation."](#)
- Install and configure Oracle Access Manager as described in [Chapter 13, "Configuring Oracle Access Manager 11g."](#)
- Install and configure Oracle HTTP Server as described in [Section 6.2, "Installing Oracle HTTP Server."](#)
- Install and configure WebGate as described in [Section 19.7, "Installing and Configuring WebGate 11g."](#)

18.4.2 Integrating Oracle Identity Federation with Oracle Access Manager in SP Mode

This section covers the following topics:

- [Section 18.4.2.1, "Configuring the Oracle Access Manager 11g SP Engine"](#)
- [Section 18.4.2.2, "Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager"](#)

18.4.2.1 Configuring the Oracle Access Manager 11g SP Engine

In SP mode, Oracle Identity Federation uses federation protocols to authenticate a user, and then requests the authentication module to create an authenticated session at Oracle Access Manager. Oracle Access Manager 11g SP engine is used for this purpose. The engine also provides logout integration. To configure the SP engine, run the `setupOIFOAMConfig` script from `IDMHOST1`.

To perform the integration proceed as follows:

1. On `IDMHOST1`, set the `DOMAIN_HOME` and `IDM_ORACLE_HOME` environment variables. Then, set the environment by running the `setOIFEnv.sh` script in the current shell. The script resides at `IDM_ORACLE_HOME/fed/scripts`.

For example:

```
export DOMAIN_HOME=/u01/app/oracle/admin/IDMDomain/aserver/IDMDomain
export IDM_ORACLE_HOME=IDM_ORACLE_HOME
cd $IDM_ORACLE_HOME/fed/scripts
. setOIFEnv.sh
```

2. Edit the file `setupOIFOAMIntegration.py`, which is located in: `IDM_ORACLE_HOME/fed/scripts/oam`

Locate the line :

```
setConfigProperty("spengines","oam11guniqueuserid","cn","string")
```

Change the line to read:

```
setConfigProperty("spengines","oam11guniqueuserid","uid","string")
```

Save the file.

3. Change Directory to `IDM_ORACLE_HOME/fed/scripts/oam`.
4. Execute the `setupOIFOAMConfig` script providing the following input parameters:

- `oifHost`: Hostname of one off the OIF managed servers
- `oifPort`: Port number of OIF Managed server
- `oifAdminHost`: Hostname of WebLogic Admin server
- `oifAdminPort`: Port number of WebLogic Admin server
- `oamAdminHost`: Hostname of WebLogic Admin Server
- `oamAdminPort`: Port number of WebLogic Admin server
- `agentType`: The agent type used, for example, `webgate11g`

For Linux, the syntax is:

```
oifHost=myhost oifPort=portnum oamAdminHost=myhost2 oamAdminPort=portnum2
agentType=webgate11g ./setupOIFOAMConfig.sh
```

For Windows, the syntax is:

```
setupOIFOAMConfig.cmd "oifHost=myhost" "oifPort=portnum" "oamAdminHost=myhost2"
"oamAdminPort=portnum2" "agentType=webgate11g"
```

For example:

```
oifHost=IDMHOST1 oifAdminHost=ADMINVHN oamAdminHost=ADMINVHN oifPort=7499
oifAdminPort=7001 oamAdminPort=7001 agentType=webgate11g ./setupOIFOAMConfig.sh
```

The script prompts you for the username and password you use to connect to the WebLogic Administration Server, for example, `weblogic`.

Sample Output:

```
Initializing WebLogic Scripting Tool (WLST) ...
Welcome to WebLogic Server Administration Scripting Shell
```

Type help() for help on available commands

```
OIF admin user : weblogic_idm
*OIF admin password:*****
OAM admin user : oamadmin
*OAM admin password:*****
Connecting to t3://ADMINVHN:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'IDMDomain'.
```

Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.

Location changed to domainRuntime tree. This is a read-only tree with DomainMBean as the root.
For more help, use help(domainRuntime)

Already in Domain Runtime Tree

Already in Domain Runtime Tree

```
Disconnected from weblogic server: AdminServer
Connecting to t3://ADMINVHN:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'IDMDomain'.
```

Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.

```
Disconnected from weblogic server: AdminServer
Connecting to t3://IDMHOST1:7499 with userid weblogic ...
Successfully connected to managed Server 'wls_oif1' that belongs to domain
'IDMDomain'.
```

Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.

```
Disconnected from weblogic server: wls_oif1
Connecting to t3://ADMINVHN:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'IDMDomain'.
```

Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.

```
Disconnected from weblogic server: AdminServer
Connecting to t3://ADMINVHN:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'IDMDomain'.
```

Warning: An insecure protocol was used to connect to the server. To ensure on-the-wire security, the SSL port or Admin port should be used instead.

Registration Successful

Disconnected from weblogic server: AdminServer

5. Restart Managed servers WLS_OIF1 and WLS_OIF2 as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

18.4.2.2 Updating the Oracle Identity Federation Authentication Scheme in Oracle Access Manager

Oracle Access Manager ships with an Oracle Identity Federation Authentication Scheme. This scheme needs to be updated before it can be used. To update the scheme, log in to the OAM console as the OAM administration user. Use the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) Then perform the following steps:

1. Click the **Policy Configuration** tab.
2. Expand **Authentication Schemes** under the Shared Components tree.
3. Select **OIFScheme** from under the Authentication Schemes and then select **Open** from the menu.
4. On the Authentication Schemes page, provide the following information
 - **Challenge URL:**
`https://sso.mycompany.com:443/fed/user/spoam11g`
 - **Context Type:** Select **external** from the list.Accept the defaults for all other values
5. Click **Apply** to update the OIFScheme.

18.4.3 Switching from Local Authentication to Federation SSO

Note: Before you perform this operation, Oracle Identity Federation must already be configured for Federation SSO with a Federation IdP, and that IdP must be set as the Default SSO IdP in the OIF Administration Console **Service Provider** section.

To switch the authentication of the Oracle Access Manager security domain from local authentication to Federation SSO, proceed as follows:

1. Log in to the OAM console as the OAM administration user.
2. Navigate to **Policy Configuration -> Authentication Schemes -> FAAuthScheme**.
3. Change **Challenge Method** from FORM to DAP.
4. Set the **Authentication Module** to DAP.
5. Change **Challenge URL** from `/pages/login.jsp` to:
`https://sso.mycompany.com:443/fed/user/spoam11g`
6. Change **Context Type** from `customWar` to `external`.
7. Set the **Challenge Parameters** field to `TAPPartnerId=OIFDAPPartner`.
8. Click **Apply**.

After you perform these steps, accessing a Fusion Applications resource protected by the FAAuthScheme triggers the Federation SSO flow and redirects the user to the IdP

for authentication. An example of such a Fusion Applications resource might be:
<https://fs.mycompany.com:443/homePage/faces/AtkHomePageWelcome>

18.5 Backing Up the Identity Management Configuration

After you have verified that the extended domain is working, back up the domain configuration. This is a quick backup for the express purpose of immediate restore in case of failures in future procedures. Back up the configuration to the local disk. This backup can be discarded once you have completed the enterprise deployment. Once you have completed the enterprise deployment, you can initiate the regular deployment-specific backup and recovery process.

For information about backing up the environment, see "Backing Up Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*. For information about recovering your information, see "Recovering Your Environment" in the *Oracle Fusion Middleware Administrator's Guide*.

To back up the configuration at this point:

1. Back up the Web tier:

- a. Shut down the instance using `opmnctl`.

```
ORACLE_BASE/admin/instance_name/bin/opmnctl stopall
```

- b. Back up the Middleware Home on the web tier using the following command (as root):

```
tar -cvpf BACKUP_LOCATION/web.tar $MW_HOME
```

- c. Back up the Instance Home on the web tier using the following command (as root):

```
tar -cvpf BACKUP_LOCATION/web_instance.tar $ORACLE_INSTANCE
```

- d. Start the instance using `opmnctl`:

```
ORACLE_BASE/admin/instance_name/bin/opmnctl startall
```

2. Back up the database. This is a full database backup (either hot or cold) using Oracle Recovery Manager (recommended) or OS tools such as `tar` for cold backups if possible.

3. Back up the Administration Server domain directory to save your domain configuration. The configuration files are located in the following directory:

```
ORACLE_BASE/admin/domain_name
```

To back up the Administration Server run the following command on OIMHOST1:

```
tar -cvpf edgdomainback.tar ORACLE_BASE/admin/domain_name
```

Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment

This chapter describes how to configure single sign-on (SSO) for administration consoles in an Identity Management Enterprise deployment.

This chapter includes the following topics:

- [Section 19.1, "Overview of Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment"](#)
- [Section 19.2, "Prerequisites"](#)
- [Section 19.3, "Create WebLogic Security Providers"](#)
- [Section 19.4, "Assigning WLSAdmins Group to WebLogic Administration Groups"](#)
- [Section 19.5, "Register EM with OPSS Security Provider"](#)
- [Section 19.6, "Updating the boot.properties File"](#)
- [Section 19.7, "Installing and Configuring WebGate 11g"](#)
- [Section 19.8, "Validating WebGate and the Oracle Access Manager Single Sign-On Setup."](#)

19.1 Overview of Configuring Single Sign-on for Administration Consoles in an Enterprise Deployment

You assign WebLogic Administration groups, update boot.properties, and restart the servers. Then you install and configure WebGate and validate the setup. After WebGate is installed and configured, the Oracle HTTP Server intercepts requests for the consoles and forwards them to Oracle Access Manager for validation

The administration consoles referred to in the chapter title are:

- Oracle Enterprise Manager Fusion Middleware Control
- Oracle WebLogic Server Administration Console
- Oracle Access Manager Console
- Oracle Identity Manager Console

19.2 Prerequisites

Before you attempt to integrate administration consoles with single sign-on, ensure that the following tasks have been performed in the IDMDomain

1. Configuring Oracle HTTP Server, as described in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment."](#)
2. Configuring Oracle Access Manager, as described in [Chapter 13, "Configuring Oracle Access Manager 11g."](#)
3. Provisioning Weblogic Administrators in LDAP as described in [Section 11.5, "Preparing the Identity Store."](#)

19.3 Create WebLogic Security Providers

This section describes how to integrate administration consoles with single sign-on. You need to perform the procedures in this section if you have placed Oracle Identity Manager into a separate domain.

This section contains the following topics:

- [Section 19.3.1, "Creating Oracle Directory Authenticator"](#)
- [Section 19.3.2, "Creating Oracle Access Manager Identity Asserter"](#)

Note: Once you have enabled single sign-on for the administration consoles, ensure that at least one OAM Server is running to enable console access.

If you have used the Oracle Weblogic console to shut down all of the Oracle Access Manager Managed Servers, then restart one of those Managed Servers manually before using the console again.

To start WLS_OAM1 manually, use the command:

```
MSERVER_HOME/bin/startManagedWeblogic.sh WLS_OAM1  
t3://ADMINVHN:7001
```

19.3.1 Creating Oracle Directory Authenticator

This section sets up a directory authenticator to enable you to use the users in your LDAP directory to access administration consoles.

You do not need to perform these steps if you have integrated Oracle Access Manager and Oracle Identity Manager as described in [Section 18.2, "Integrating Oracle Identity Manager and Oracle Access Manager 11g."](#)

1. Log in to the WebLogic Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click **Security Realms** from the Domain structure menu.
3. Click **Lock and Edit** in the Change Center.
4. Click **myrealm**.
5. Select the **Providers** tab.
6. Click **DefaultAuthenticator**.
7. Set **Control Flag** to **SUFFICIENT**.

8. Click **Save**.
9. Click **Security Realms** from the Domain structure menu.
10. Click **myrealm**.
11. Select the **Providers** tab.
12. Click **New**.
13. Supply the following information if you are using Oracle Virtual Directory:
 For Oracle Virtual Directory:
 - **Name:** OVDAuthenticator
 - **Type:** OracleVirtualDirectoryAuthenticator
 For Oracle Internet Directory:
 - **Name:** OIDAAuthenticator
 - **Type:** OracleInternetDirectoryAuthenticator
14. Click **OK**.
15. Click **OVDAuthenticator** or **OIDAAuthenticator**.
16. Set **Control Flag** to **SUFFICIENT**.
17. Click **Save**.
18. Select the **Provider Specific** tab.
19. Enter the following details:
 - **Host:** idstore.mycompany.com
 - **Port:** 389
 - **Principal:** cn=oamLDAP,cn=Users,dc=us,dc=mycompany,dc=com
 - **Credential:** oamLDAP password
 - **Confirm Credential:** oamLDAP password
 - **User Base DN:** cn=Users,dc=mycompany,dc=com
 - **All Users Filter:** (&(uid=*)(objectclass=person))
 - **User From Name Filter:** (&(uid=%u)(objectclass=person))
 - **User Name Attribute:** uid
 - **Group Base DN:** cn=Groups,dc=mycompany,dc=com
 - **GUID Attribute:** orclguid
20. Click **Save**.
21. Click **Activate Changes** from the **Change Center**.
22. Restart WebLogic Administration Server and all the Managed Servers, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

Validating the Configuration

Validate the configuration by logging in to the OAM console as the user oamadmin.

You can perform a further validation test by using the Oracle WebLogic Administration Console, as follows.

1. Log in to the WebLogic Administration console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Select **Security Realms** from the Domain structure menu.
3. Click **myrealm**.
4. Click the **Users and Groups** tab.
5. Click **Users**.
LDAP users are displayed.

19.3.2 Creating Oracle Access Manager Identity Asserter

This section sets up an Oracle Access Manager asserter to enable you to delegate responsibility for credential collection to Oracle Access Manager.

You do not need to perform these steps if you have Integrated Oracle Access Manager and Oracle Identity Manager as described in [Section 18.2, "Integrating Oracle Identity Manager and Oracle Access Manager 11g."](#)

1. Log in to the WebLogic Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click **Security Realms** from the Domain structure menu.
3. Click **Lock and Edit** in the **Change Center**.
4. Click **myrealm**.
5. Select the **Providers** tab.
6. Click **New**.
7. Supply the following information:
 - **Name:** OAMIDAsserter
 - **Type:** OAMIdentityAsserter
8. Click **OK**.
9. Click **OAMIDAsserter**.
10. Set **Control Flag** to **REQUIRED**.
11. Click **Save**.
12. Click **Security Realms** from the Domain structure menu
13. Click **myrealm**.
14. Select the **Providers** tab.
15. Click **Reorder**.
16. Using the arrows on the right hand side order the providers such that the order is:
 - **OAMIDAsserter**
 - **Default Authenticator**
 - **OVDAuthenticator** or **OIDAuthenticator**
 - **Default Identity Asserter**

Note: Oracle Identity Manager providers only exist if Oracle Identity Manager has been configured.

17. Click **OK**.
18. Click **Activate Changes**.
19. Restart WebLogic Administration Server and all the Managed Servers, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

19.4 Assigning WLSAdmins Group to WebLogic Administration Groups

In an enterprise, it is typical to have a centralized Identity Management domain where all users, groups and roles are provisioned and multiple application domains (such as a SOA domain and WebCenter Portal domain). The application domains are configured to authenticate using the central Identity Management domain.

In [Section 11.5, "Preparing the Identity Store"](#) you created a user called `weblogic_idm` and assigned it to the group WLSAdmins. To be able to manage WebLogic using this account you must add the WLSAdmins group to the list of WebLogic Administration groups. This section describes how to add the WLSAdmins Group to the list of WebLogic Administrators.

Perform this step for each domain in the topology.

If you are using a split domain topology, perform these tasks on both IDMDomain and OIMDomain.

1. Log in to the WebLogic Administration Server Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. In the left pane of the console, click **Security Realms**.
3. On the Summary of Security Realms page, click **myrealm** under the **Realms** table.
4. On the Settings page for myrealm, click the **Roles & Policies** tab.
5. On the Realm Roles page, expand the **Global Roles** entry under the **Roles** table. This brings up the entry for Roles. Click the **Roles** link to go to the Global Roles page.
6. On the Global Roles page, click the **Admin** role to go to the Edit Global Role page:
 - a. On the Edit Global Roles page, under the **Role Conditions** table, click the **Add Conditions** button.
 - b. On the Choose a Predicate page, select **Group** from the drop down list for predicates and click **Next**.
 - c. On the Edit Arguments Page, Specify **IDM Administrators** in the **Group Argument** field and click **Add**.
7. Click **Finish** to return to the Edit Global Rule page.
8. The **Role Conditions** table now shows the IDM Administrators Group as an entry.
9. Click **Save** to finish adding the Admin role to the IDM Administrators Group.
10. Validate that the changes were successful by bringing up the WebLogic Administration Server Console using a web browser. Log in using the credentials for the `weblogic_idm` user.

19.5 Register EM with OPSS Security Provider

If you are using a split domain you must register the Oracle Enterprise Manager Fusion Middleware Control application with the OPSS policy store in order for logout to work correctly in the IDMDomain. This is not necessary in the OIMDomain.

To register Fusion Middleware Control, proceed as follows.

1. Start WLST using the command:

```
MW_HOME/oracle_common/common/bin/wlst.sh
```

2. Connect to the IDMDomain using the WLST connect() command, as follows:

```
connect()
Enter User Name: weblogic
Password: password_for_account
Server URL: t3://adminvhn.mycompany.com:7001
```

3. Run the command:

```
addOAMSSOProvider(loginuri="/em/adfAuthentication",
logouturi="/oamsso/logout.html", autologinuri="/obrar.cgi")
```

4. Exit WLST using the command:

```
exit()
```

5. Restart the admin server and the managed servers wls_oam1 and wls_oam2 as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

19.6 Updating the boot.properties File

Update the boot.properties file for the Administration Server and the managed servers with the WebLogic admin user created in Oracle Internet Directory.

This section contains the following topics:

- [Section 19.6.1, "Update the Administration Server on IDMHOST1"](#)
- [Section 19.6.2, "Update the Administration Server on OIMHOST1"](#)
- [Section 19.6.3, "Restarting the Servers"](#)

19.6.1 Update the Administration Server on IDMHOST1

1. On IDMHOST1, go the directory:

```
ORACLE_BASE/admin/domainName/aserver/domainName/servers/serverName/security
```

For example:

```
cd ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain/servers/AdminServer/security
```

2. Rename the existing boot.properties file.
3. Use a text editor to create a file called boot.properties under the security directory. Enter the following lines in the file:

```
username=adminUser
password=adminUserPassword
```

For example:


```
username=weblogic_idm
password=Password for weblogic_idm user
```

Note: When you start the Administration Server, the username and password entries in the file get encrypted.

For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

19.6.2 Update the Administration Server on OIMHOST1

For a split domain topology, you must also perform these steps on OIMHOST1.

1. On OIMHOST1, go to the directory:

```
ORACLE_BASE/admin/domainName/aserver/domainName/servers/serverName/security
```

For example:

```
cd ORACLE_BASE/admin/OIMDomain/aserver/OIMDomain/servers/AdminServer/security
```

2. Rename the existing `boot.properties` file.
3. Use a text editor to create a file called `boot.properties` under the security directory. Enter the following lines in the file:

```
username=adminUser
password=adminUserPassword
```

For example:

```
username=weblogic_idm
password=Password for weblogic_idm user
```

Note: When you start the Administration Server, the username and password entries in the file get encrypted.

For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

19.6.3 Restarting the Servers

Restart the WebLogic Administration server and all managed servers, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

19.7 Installing and Configuring WebGate 11g

This section describes how to install and configure WebGate.

This section contains the following topics:

- [Section 19.7.1, "Prerequisites"](#)
- [Section 19.7.2, "Making Special gcc Libraries Available"](#)
- [Section 19.7.3, "Installing Oracle WebGate on WEBHOST1 and WEBHOST2"](#)

19.7.1 Prerequisites

Ensure that the following tasks have been performed before installing the Oracle Web Gate:

1. Install and configure the Oracle Web Tier as described in [Chapter 7](#).
2. Ensure Oracle Access Manager has been configured as described in [Chapter 13](#).

19.7.2 Making Special gcc Libraries Available

Oracle Web Gate requires special versions of gcc libraries to be installed (Linux only). These library files must exist somewhere on the Linux system. The Web Gate installer asks for the location of these library files at install time. Download the libraries from <http://gcc.gnu.org>, as described in "Installing Third-Party GCC Libraries (Linux and Solaris Operating Systems Only)" in *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*

19.7.3 Installing Oracle WebGate on WEBHOST1 and WEBHOST2

Before starting the installer ensure that Java is installed on your machine.

1. Start the WebGate installer by issuing the command:

```
./runInstaller
```

You are asked to specify the location of the Java Development Kit for example:

```
MW_HOME/jrockit_version
```

2. On the Welcome screen, click **Next**.
3. On the Prerequisites screen, after all the checks have successfully completed, click **Next**.
4. On the Installation Location Screen, enter the following information:
 - **Oracle Middleware Home:** /u01/app/oracle/product/fmw
 - **Oracle Home Directory:** webgate

`MW_HOME/webgate` is defined as `WEBGATE_ORACLE_HOME`

Click **Next**.

5. Specify the location of the GCC runtime libraries, for example:
/u01/app/oracle/oam_lib.

Click **Next**.

6. On the installation summary screen, click **Install**.
7. Click **Next**.
8. Click **Finish**.

Deploy WebGate to Oracle HTTP, as follows:

1. Execute the command `deployWebGate` which is located in:

```
WEBGATE_ORACLE_HOME/webgate/ohs/tools/deployWebGate
```

The command takes the following arguments:

Oracle HTTP Instance configuration Directory

WebGate Home Directory

For example:

```
./deployWebGateInstance.sh -w ORACLE_INSTANCE/config/OHS/ohs1 -oh WEBGATE_
ORACLE_HOME
```

2. Set the library path and change directory.

On Linux systems, set the library path to include the `WEB_ORACLE_HOME/lib` directory, for example:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:WEB_ORACLE_HOME/lib
```

On Windows, set the `WEBGATE_ORACLE_HOME\webgate\ohs\lib` location and the `WEB_ORACLE_HOME\bin` location in the `PATH` environment variable. Add a semicolon (;) followed by this path at the end of the entry for the `PATH` environment variable.

Change directory:

On Linux, change directory to: `WEBGATE_ORACLE_HOME/webgate/ohs/tools/setup/InstallTools`

On Windows, change directory to: `WEBGATE_ORACLE_HOME\webgate\ohs\tools\EditHttpConf`

3. Run the following command to copy the file `apache_webgate.template` from the WebGate home directory to the WebGate instance location (renamed to `webgate.conf`) and update the `httpd.conf` file to add one line to include the name of `webgate.conf`.

On Linux, type:

```
./EditHttpConf -w ORACLE_INSTANCE/config/OHS/component_name -oh WEBGATE_ORACLE_
HOME
```

On Windows, type:

```
EditHttpConf.exe -w ORACLE_INSTANCE\config\OHS\component_name -oh WEBGATE_
ORACLE_HOME
```

4. Copy the files `ObAccessClient.xml`, `cwallet.sso`, and `password.xml`, which were generated when you created the agent from the directory `ASERVER_HOME/domain_name/output/Webgate_IDM_11g` on `IDMHOST1`, to the directory `ORACLE_INSTANCE/config/OHS/component/webgate/config`.
5. The files `aaa_key.pem` and `aaa_cert.pem` were generated when you created the agent from the directory `ASERVER_HOME/output/Agent_11g Name` on `IDMHOST1`. Copy the files `aaa_key.pem` and `aaa_cert.pem` to the WebGate instance directory `OHS_INSTANCE_HOME/config/OHS/component/webgate/config/simple`.
6. Restart the Oracle HTTP Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

19.8 Validating WebGate and the Oracle Access Manager Single Sign-On Setup

To validate that WebGate is functioning correctly, open a web browser and go the OAM console URL listed in [Section 20.2, "About Identity Management Console URLs."](#)

You now see the Oracle Access Manager Login page displayed. Enter your OAM administrator user name (for example, `oamadmin`) and password and click **Login**. Then you see the Oracle Access Manager console displayed.

To validate the single sign-on setup, open a web browser and go the WebLogic Administration Console and to Oracle Enterprise Manager Fusion Middleware Control at the URLs listed in [Section 20.2, "About Identity Management Console URLs."](#)

The Oracle Access Manager Single Sign-On page displays. Provide the credentials for the `weblogic_idm` user to log in.

Managing the Topology for an Enterprise Deployment

This chapter describes some operations that you can perform after you have set up the Identity Management topology. These operations include monitoring, scaling, backing up your topology, and troubleshooting.

This chapter includes the following topics:

- [Section 20.1, "Starting and Stopping Oracle Identity Management Components"](#)
- [Section 20.2, "About Identity Management Console URLs"](#)
- [Section 20.3, "Monitoring Enterprise Deployments"](#)
- [Section 20.4, "Scaling Enterprise Deployments"](#)
- [Section 20.5, "Auditing Identity Management"](#)
- [Section 20.6, "Performing Backups and Recoveries"](#)
- [Section 20.7, "Patching Enterprise Deployments"](#)
- [Section 20.8, "Preventing Timeouts for SQL"](#)
- [Section 20.9, "Troubleshooting"](#)

20.1 Starting and Stopping Oracle Identity Management Components

This section describes how to start, stop and restart the various components of the Oracle Enterprise Deployment for Identity Management.

This section contains the following topics:

- [Section 20.1.1, "Startup Order"](#)
- [Section 20.1.2, "Starting and Stopping Oracle Virtual Directory"](#)
- [Section 20.1.3, "Starting and Stopping Oracle Internet Directory"](#)
- [Section 20.1.4, "Starting, Stopping, and Restarting Oracle HTTP Server"](#)
- [Section 20.1.5, "Starting and Stopping Node Manager"](#)
- [Section 20.1.6, "Starting, Stopping, and Restarting WebLogic Administration Server"](#)
- [Section 20.1.7, "Starting, Stopping, and Restarting Oracle Identity Manager"](#)
- [Section 20.1.8, "Starting, Stopping, and Restarting Oracle Access Manager Managed Servers"](#)

- [Section 20.1.9, "Starting and Stopping Oracle Identity Federation Managed Servers"](#)

20.1.1 Startup Order

When starting up your entire infrastructure, start the components in the following order, (ignoring those not in your topology):

1. Database(s)
2. Database Listener(s)
3. Oracle Internet Directory
4. Oracle Virtual Directory
5. Oracle Access Manager Server(s)
6. WebLogic Administration Server
7. Oracle HTTP Server(s)
8. SOA Server(s)
9. Oracle Identity Manager Server(s)

20.1.2 Starting and Stopping Oracle Virtual Directory

Start and stop Oracle Virtual Directory as follows.

20.1.2.1 Starting Oracle Virtual Directory

Start system components such as Oracle Virtual Directory by typing:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

20.1.2.2 Stopping Oracle Virtual Directory

Stop system components such as Oracle Virtual Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

20.1.3 Starting and Stopping Oracle Internet Directory

Start and stop Oracle Internet Directory as follows.

20.1.3.1 Starting Oracle Internet Directory

Start system components such as Oracle Internet Directory by typing

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the system components have started by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

20.1.3.2 Stopping Oracle Internet Directory

Stop system components such as Oracle Internet Directory by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

20.1.4 Starting, Stopping, and Restarting Oracle HTTP Server

Prior to starting/stopping the Oracle HTTP server ensure that the environment variables `WEB_ORACLE_HOME` and `ORACLE_INSTANCE` are defined and that `ORACLE_HOME/opmn/bin` appears in the `PATH`. For example:

```
export ORACLE_HOME=WEB_ORACLE_HOME
export ORACLE_INSTANCE=/u01/app/oracle/admin/web[1-2]
export PATH=$ORACLE_HOME/opmn/bin:$PATH
```

20.1.4.1 Starting Oracle HTTP Server

Start the Oracle web tier by issuing the command:

```
opmnctl startall
```

20.1.4.2 Stopping Oracle HTTP Server

Stop the web tier by issuing the command

```
opmnctl stopall
```

to stop the entire Web tier or

```
opmnctl stopproc process-type=OHS
```

to stop Oracle HTTP Server only.

20.1.4.3 Restarting Oracle HTTP Server

You can restart the web tier by issuing a Stop followed by a Start as described in the previous sections.

To restart the Oracle HTTP server only, use the following command.

```
opmnctl restartproc process-type=OHS
```

20.1.5 Starting and Stopping Node Manager

Start and stop the Node Manager as follows:

20.1.5.1 Starting Node Manager

If the Node Manager being started is the one that controls the Administration Server (IDMHOST1 or IDMHOST2), then prior to starting the Node Manager issue the command:

```
export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
```

To start Node Manager, issue the commands:

```
cd ORACLE_BASE/product/fmw/wlserver_10.3/server/bin
./startNodeManager.sh
```

20.1.5.2 Stopping Node Manager

To stop Node Manager, kill the process started in the previous section.

20.1.5.3 Starting Node Manager for an Administration Server

```
cd ORACLE_BASE/product/fmw/wlserver_10.3/server/bin
export JAVA_OPTIONS=-DDomainRegistrationEnabled=true
./startNodeManager.sh
```

Note: It is important to set `-DDomainRegistrationEnabled=true` whenever you start a Node Manager that manages the Administration Server.

20.1.6 Starting, Stopping, and Restarting WebLogic Administration Server

Start and stop the WebLogic Administration Server as described in the following sections.

Note: `Admin_user` and `Admin_Password` are only used to authenticate connections between Node Manager and clients. They are independent from the server administration ID and password and are stored in the `ORACLE_BASE/admin/domain_name/aserver/domain_name/config/nodemanager/nm_password.properties` file.

20.1.6.1 Starting WebLogic Administration Server

The recommended way to start the Administration server is to use WLST and connect to Node Manager:

```
cd ORACLE_BASE/product/fmw/oracle_common/common/bin
./wlst.sh
```

Once in WLST shell, execute

```
nmConnect('Admin_User','Admin_Password','ADMINHOST1','5556',
'IDMDomain','/u01/app/oracle/admin/domain_name/aserver/IDMDomain')
nmStart('AdminServer')
```

Alternatively, you can start the Administration server by using the command:

```
DOMAIN_HOME/bin/startWeblogic.sh
```

20.1.6.2 Stopping WebLogic Administration Server

To stop the Administration Server, log in to the WebLogic console using the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select **AdminServer(admin)**.
4. Click **Shutdown** and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you want to shut down the Administration Server.

20.1.6.3 Restarting WebLogic Administration Server

Restart the server by following the **Stop** and **Start** procedures in the previous sections.

20.1.7 Starting, Stopping, and Restarting Oracle Identity Manager

Start and stop Oracle Identity Manager and Oracle SOA Suite servers as follows:

20.1.7.1 Starting Oracle Identity Manager

To start the Oracle Identity Manager Managed Server(s), log in to the WebLogic console using the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select **SOA Servers (WLS_SOA1 and/or WLS_SOA2)**.

Note: You can start the Oracle Identity Manager and Oracle SOA Suite servers independently of each other. There is no dependency in their start order. However, the SOA server must be up and running for all of the Oracle Identity Manager functionality to be available.

4. Click the **Start** button.
5. Click **Yes** when asked to confirm that you want to start the server(s).
6. After WLS_SOA1 and/or WLS_SOA2 have started, select WLS_OIM1 and/or WLS_OIM2
7. Click **Start**.
8. Click **Yes** when asked to confirm that you want to start the server(s).

20.1.7.2 Stopping Oracle Identity Manager

To stop the Oracle Identity Manager Managed Server(s), log in to the WebLogic console using the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select **OIM Servers (WLS_OIM1 and/or WLS_OIM2)** and **(WLS_SOA1 and/or WLS_SOA2)**.
4. Click the **Shutdown** button and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you want to shutdown the server(s).

20.1.7.3 Restarting Oracle Identity Manager

Restart the server by following the **Stop** and **Start** procedures in the previous sections.

20.1.8 Starting, Stopping, and Restarting Oracle Access Manager Managed Servers

Start and stop Oracle Access Manager Managed Servers as follows:

20.1.8.1 Starting Oracle Access Manager Managed Servers

To start the Oracle Access Manager Managed Server(s), log in to the WebLogic console using the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**.
4. Click the **Start** button.
5. Click **Yes** when asked to confirm that you want to start the server(s).

20.1.8.2 Stopping Oracle Access Manager Managed Servers

To stop the Oracle Access Manager Managed Server(s), log in to the WebLogic console using the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)

Then proceed as follows:

1. Select **Environment - Servers** from the Domain Structure menu.
2. Click the **Control** tab.
3. Select **OAM Servers (WLS_OAM1 and/or WLS_OAM2)**.
4. Click the **Shutdown** button and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

20.1.8.3 Restarting Oracle Access Manager Managed Servers

Restart the server by following the **Stop** and **Start** procedures in the previous sections.

20.1.9 Starting and Stopping Oracle Identity Federation Managed Servers

Start and stop Oracle Identity Federation Managed Servers as follows:

20.1.9.1 Starting Oracle Identity Federation

To start the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)

Then proceed as follows:

1. Select **Environment - Servers** from the **Domain Structure** menu.
2. Click the **Control** tab.
3. Select **OIF Servers (WLS_OIF1 and/or WLS_OIF2)**.
4. Click **Start**.
5. Click **Yes** when asked to confirm that you want to start the server(s).

20.1.9.2 Stopping Oracle Identity Federation

To stop the Oracle Identity Federation Managed Server(s), log in to the WebLogic console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) Then proceed as follows:

1. Select **Environment - Servers** from the **Domain Structure** menu.
2. Click the **Control** tab.
3. Select **OIF Servers (WLS_OIF1 and/or WLS_OIF2)**.
4. Click **Shutdown** and select **Force Shutdown now**.
5. Click **Yes** when asked to confirm that you want to shut down the server(s).

20.1.9.3 Restarting Oracle Identity Federation

Restart the server by following the previous Stop and Start procedures.

20.1.9.4 Starting the EMAgent

Start the EMAgent by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl startall
```

You can verify that the instance started successfully by executing:

```
ORACLE_INSTANCE/bin/opmnctl status -l
```

20.1.9.5 Stopping the Oracle Identity Federation Instances and EMAgent

Stop the Oracle Identity Federation Instance and EMAgent by executing the following command:

```
ORACLE_INSTANCE/bin/opmnctl stopall
```

20.2 About Identity Management Console URLs

[Table 20–1](#) lists the administration consoles used in this guide and their URLs.

Table 20–1 Console URLs

Domain	Console	URL
IDMDomain	WebLogic Administration Console	http://admin.mycompany.com/console
IDMDomain	Enterprise Manager FMW Control	http://admin.mycompany.com/em
IDMDomain	OAM Console	http://admin.mycompany.com/oamconsole
IDMDomain	ODSM	http://admin.mycompany.com/odsm
OIMDomain	OIM Console	https://sso.mycompany.com/oim
OIMDomain	WebLogic Administration Console	http://oimadmin.mycompany.com/console
OIMDomain	Enterprise Manager FMW Control	http://oimadmin.mycompany.com/em

20.3 Monitoring Enterprise Deployments

This section provides information about monitoring the Identity Management enterprise deployment described in this manual.

This section contains the following topics:

- [Section 20.3.1, "Monitoring Oracle Internet Directory"](#)
- [Section 20.3.2, "Monitoring Oracle Virtual Directory"](#)
- [Section 20.3.3, "Monitoring WebLogic Managed Servers"](#)

20.3.1 Monitoring Oracle Internet Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Internet Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.
2. The Identity and Access section below the chart includes the name of each individual Oracle Internet Directory instance (for example: oid1, oid2), its status, host name, and CPU usage percentage. A green arrow in the Status column indicates that the instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Internet Directory instance to view the home page for that instance.
3. The home page for an instance displays metrics for the instance such as performance, load, security, response, CPU utilization %, and memory utilization %.

20.3.1.1 Oracle Internet Directory Component Names Assigned by Oracle Identity Manager Installer

When you perform an Oracle Internet Directory installation using Oracle Identity Management 11g Installer, the default component name that the installer assigns to the Oracle Internet Directory instance is oid1. You cannot change this component name.

The instance specific configuration entry for this Oracle Internet Directory instance is `cn=oid1, cn=osldldapd, cn=subconfigsubentry`.

If you perform a second Oracle Internet Directory installation on another computer and that Oracle Internet Directory instance uses the same database as the first instance, the installer detects the previously installed Oracle Internet Directory instance on the other computer using the same Oracle database, so it gives the second Oracle Internet Directory instance a component name of `oid2`.

The instance specific configuration entry for the second Oracle Internet Directory instance is `cn=oid2, cn=osldldapd, cn=subconfigsubentry`. A change of properties in the entry `cn=oid2, cn=osldldapd, cn=subconfigsubentry` does not affect the first instance (`oid1`).

If a third Oracle Internet Directory installation is performed on another computer and that instance uses the same database as the first two instances, the installer gives the third Oracle Internet Directory instance a component name of `oid3`, and so on for additional instances on different hosts that use the same database.

Note that the shared configuration for all Oracle Internet Directory instances is `cn=dsainfo, cn=configsets, cn=oracle internet directory`. A change in this entry affects all the instances of Oracle Internet Directory.

This naming scheme helps alleviate confusion when you view your domain using Oracle Enterprise Manager by giving different component names to your Oracle Internet Directory instances.

20.3.2 Monitoring Oracle Virtual Directory

You can use the Oracle Enterprise Manager Fusion Middleware Control to monitor Oracle Virtual Directory, as follows:

1. On the Farm home page for an Identity Management domain, view the Fusion Middleware pie chart. This chart shows the status of Oracle Fusion Middleware components. Green sections of the chart indicate components that are up and running properly, and red sections indicate components that are down.
2. The Identity and Access section below the chart includes the name of each instance of the Oracle Virtual Directory application (for example, ovd1, ovd2), its status, and host name. A green arrow in the Status column indicates that the Oracle Virtual Directory instance is up and running properly, and a red arrow indicates the instance is down. Click the name of an individual Oracle Virtual Directory instance to view the home page for that instance.
3. The home page for an instance displays metrics and configurations for the instance such as:
 - Oracle Virtual Directory status - A green arrow next to the Oracle Virtual Directory instance name at the top of the page indicates that the instance is up and running properly and a red arrow indicates that the instance is down.
 - Current Load - This indicates the current work load of this Oracle Virtual Directory instance. It includes three metrics: Open Connections, Distinct Connected Users, and Distinct Connected IP Addresses.
 - Average Response Time Metric - This displays the average time (in milliseconds) to complete an LDAP search request.
 - Operations Metric - This displays the average number of LDAP search requests finished per millisecond.
 - Listeners - This table lists the listeners configured for this Oracle Virtual Directory instance to provide services to clients.
 - Adapters - This table lists existing adapters configured with the Oracle Virtual Directory instance. Oracle Virtual Directory uses adapters to connect to different underlying data repositories.
 - Resource Usage - On the right hand side of the page, the CPU and memory utilization metrics are displayed to indicate the system resources consumed by the Oracle Virtual Directory instance.

20.3.3 Monitoring WebLogic Managed Servers

You can use Oracle Enterprise Manager Fusion Middleware Control to monitor Managed Servers and other Fusion Middleware components, such as Oracle Access Manager, Oracle Identity Manager, Oracle Identity Federation, and SOA. For more information, see the administrator guides listed in the Preface under "[Related Documents](#)" on page xix.

20.4 Scaling Enterprise Deployments

The reference enterprise topology discussed in this manual is highly scalable. It can be scaled up and or scaled out. When the topology is scaled up, a new server instance is added to a node already running one or more server instances. When the topology is scaled out, new servers are added to new nodes.

This section contains the following topics:

- [Section 20.4.1, "Scaling Up the Topology"](#)
- [Section 20.4.2, "Scaling Out the Topology"](#)

20.4.1 Scaling Up the Topology

The Oracle Identity Management topology described in the guide has three tiers: the directory tier, application tier and web tier. The components in all the three tiers can be scaled up by adding a new server instance to a node that already has one or more server instances running.

The procedures described in this section show you how to create a new managed server or directory instance. If you add a new managed server, after adding the managed server you must update your Oracle HTTP Server configuration files (on all nodes) and add the new server to the existing WebLogic cluster directives.

For example if you add a new Oracle Access Manager server, you must update `sso_vh.conf` to include the new managed server.

Update `sso_vh.conf` as follows:

```
<Location /oam>
    SetHandler weblogic-handler
    WebLogicCluster
IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100, IDMHOST3.mycompany.com:14100
</Location>
```

Once you have updated `sso_vh.conf`, restart the Oracle HTTP server(s) as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#) Oracle recommends that you do this sequentially to prevent loss of service.

This section contains the following topics:

- [Section 20.4.1.1, "Scaling Up the Directory Tier"](#)
- [Section 20.4.1.2, "Scaling Up the Application Tier"](#)
- [Section 20.4.1.3, "Scaling Up the Web Tier"](#)

20.4.1.1 Scaling Up the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled up on one or both the nodes.

20.4.1.1.1 Scaling Up Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Internet Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Internet Directory instance.

To add a new Oracle Internet Directory instance to either Oracle Internet Directory node, follow the steps in [Section 9.4.2, "Configuring an Additional Oracle Internet Directory Instance"](#) with the following variations:

1. In step 2 and step 4, choose ports other than 389 and 636 since these ports are being used by the existing Oracle Internet Directory instance on the node.
2. Follow the steps in [Section 9.5.1, "Registering Oracle Internet Directory with the WebLogic Server Domain \(IDMDomain\)"](#) to register the new Oracle Internet Directory instance with the WebLogic domain. Use the location for the new Oracle Internet Directory instance as the value for `ORACLE_INSTANCE`.
3. Configure SSL server-authentication mode for the new instance as described in [Section 9.5.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections."](#)
4. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.
5. Register the new Oracle HTTP Server instance as described in [Section 9.5.1, "Registering Oracle Internet Directory with the WebLogic Server Domain \(IDMDomain\)."](#)

20.4.1.1.2 Scaling Up Oracle Virtual Directory The directory tier has two nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Virtual Directory instance. The existing Oracle Identity Management binaries on either node can be used for creating the new Oracle Virtual Directory instance.

To add a new Oracle Virtual Directory instance to either Oracle Virtual Directory node, follow the steps in [Section 12.3.2, "Configuring an Additional Oracle Virtual Directory"](#) with the following variations:

1. In step 2 and step 4, choose ports other than 6501 and 7501 since these ports are being used by the existing Oracle Virtual Directory instance on the node.
2. Follow the steps in these sections to register the new Oracle Virtual Directory instance with the WebLogic domain. Use the location for the new Oracle Virtual Directory instance as the value for `ORACLE_INSTANCE`.
 - [Section 12.4, "Post-Configuration Steps"](#)
 - [Section 12.6, "Validating the Oracle Virtual Directory Instances"](#)
 - [Section 12.7, "Creating ODSM Connections to Oracle Virtual Directory"](#)
 - [Section 12.8, "Creating Adapters in Oracle Virtual Directory"](#)
3. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

20.4.1.2 Scaling Up the Application Tier

The application tier consists of several nodes in pairs, depending on the products installed. These application servers run WebLogic Managed servers.

Some of the procedures described in this section show you how to create a new WebLogic managed server. If you add a new managed server to your topology, after adding the managed server you must update your Oracle HTTP Server configuration files (on all nodes) and add the new server to the existing WebLogic cluster directives.

For example if you add a new Oracle Access Manager server, you must update `sso_vh.conf` to include the new managed server.

Update `sso_vh.conf` as follows:


```
<Location /oam>
SetHandler weblogic-handler
WebLogicCluster
IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100, IDMHOST3.mycompany.com:1
4100
</Location>
```

Once you have updated `sso_vh.conf`, restart the Oracle HTTP server(s) as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#) Oracle recommends that you do this sequentially to prevent loss of service.

20.4.1.2.1 Scaling Up ODSM The application tier already has a node (IDMHOST2) running a Managed Server configured with Oracle Directory Services Manager components. The node contains a WebLogic Server home and an Oracle Fusion Middleware Identity Management Home on the local disk.

The existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) can be used for creating a new Managed Server for the Oracle Directory Services Manager component.

1. Follow the steps in [Section 10.4, "Expanding the ODSM Cluster."](#)
2. Be sure to choose a port other than 7499, which is already in use.
3. Reconfigure the Oracle HTTP Server module with the new Managed Server. Follow the instructions in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment"](#) to complete this task.

20.4.1.2.2 Scaling Up Oracle Access Manager 11g Scale up Oracle Access Manager as follows:

Log in to the Oracle WebLogic Server Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)

1. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
2. Click **Lock & Edit** from the Change Center menu.
3. Select an existing server on the host you want to extend, for example: `WLS_OAM1`.
4. Click **Clone**.
5. Enter the following information:
 - **Server Name:** A new name for the server, for example: `WLS_OAM3`.
 - **Server Listen Address:** The name of the host on which the Managed Server runs.
 - **Server Listen Port:** The port the new Managed Server uses. This port must be unique within the host.
6. Click **OK**.
7. Click the newly created server **WLS_OAM3**
8. Click **Save**.
9. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_OAM3` Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for

the communication between the Oracle WebLogic Administration Server and the Node Manager in `IDMHOSTn`.

If the source server from which the new one was cloned had already disabled host name verification, these steps are not required, as the host name verification settings were propagated to the cloned server. To disable host name verification:

- a. In Oracle Enterprise Manager Fusion Middleware Control, select **Oracle WebLogic Server Administration Console**.
- b. Expand the **Environment** node in the Domain Structure window.
- c. Click **Servers**. The Summary of Servers page appears.
- d. Select **WLS_OAM3** in the Names column of the table. The Settings page for server appears.
- e. Click the **SSL** tab.
- f. Click **Advanced**.
- g. Set **Hostname Verification** to **None**.
- h. Click **Save**.

10. Click **Activate configuration** from the Change Center menu.

Register the new Managed Server with Oracle Access Manager. You now must configure the new Managed Server now as an Oracle Access Manager server. You do this from the Oracle OAM console. Proceed as follows:

1. Log in to the OAM console as the `oamadmin` user. Use the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.
5. Enter the following information:
 - **Server Name:** `WLS_OAM3`
 - **Host:** Host that the server runs on
 - **Port:** Listen port that was assigned when the Managed Server was created
 - **OAM Proxy Port:** Port you want the Oracle Access Manager proxy to run on. This is unique for the host
 - **Proxy Server ID:** `AccessServerConfigProxy`
 - **Mode:** Set to `Open` or `Simple`, depending on the mode your existing Oracle Access Manager servers are operating in.
6. Click **Coherence** tab.
Set **Local Port** to a unique value on the host.
7. Click **Apply**.
8. Restart the WebLogic Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

Add the newly created Oracle Access Manager server to all WebGate Profiles that might be using it, such as `Webgate_IDM` and `IAMSuiteAgent`

For example, to add the Oracle Access Manager server to `Webgate_IDM`, access the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) Then proceed as follows:

1. Log in as the Oracle Access Manager Admin User you created in [Section 11.5, "Preparing the Identity Store."](#)
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings - SSO Agents - OAM Agents**.
4. Click the open folder icon, then click **Search**.
You should see the WebGate agent **Webgate_IDM**.
5. Click the agent **Webgate_IDM**.
6. Select **Edit** from the **Actions** menu.
7. Click **+** in the **Primary Server** list (or the **Secondary Server** list if this is a secondary server).
8. Select the newly created managed server from the **Server** drop down list.
9. Set **Max Connections** to 4.
10. Click **Apply**.

Repeat Steps 5 through 10 for **IAMSuiteAgent** and all other WebGates that might be in use.

Update the Web Tier. Once the new Managed Server has been created and started, the web tier starts to direct requests to it. Best practice, however, is to inform the web server that the new Managed Server has been created.

You do this by updating the file `sso_vh.conf` on each of the web tiers. This file resides in the directory: `ORACLE_INSTANCE/config/OHS/component name/moduleconf`.

Add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /oam>
  SetHandler weblogic-handler
  WebLogicCluster IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100
</Location>
```

```
<Location /fusion_apps>
  SetHandler weblogic-handler
  WebLogicCluster IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100
</Location>
```

to:

```
<Location /oam>
  SetHandler weblogic-handler
  WebLogicCluster
IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100, IDMHOST1.mycompany.com:14101
</Location>
```

```
<Location /fusion_apps>
  SetHandler weblogic-handler
  WebLogicCluster
IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100, IDMHOST3.mycompany.com:14100
4100
```

</Location>

Save the file and restart the Oracle HTTP server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

You can now start the new Managed Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

20.4.1.2.3 Scaling Up Oracle Identity Manager (Adding Managed Servers to Existing Nodes) In this case, you already have a node that runs a Managed Server configured with Oracle SOA Suite and Oracle Identity Manager components. The node contains a Middleware home, a SOA Oracle home, an Oracle Identity Manager Oracle home, and a domain directory for existing Managed Servers.

You can use the existing installations (the Middleware home, and domain directories) for creating new WLS_OIM and WLS_SOA servers. There is no need to install the Oracle Identity and Access Management or Oracle SOA Suite binaries in a new location, or to run pack and unpack.

Follow these steps for scaling up the topology:

1. Log in to the Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) Clone either the **WLS_OIM1** or the **WLS_SOA1** into a new Managed Server. The source Managed Server to clone should be one that already exists on the node where you want to run the new Managed Server.

To clone a Managed Server:

- a. Select **Environment** -> **Servers** from the Administration Console.
- b. From the Change Center menu, click **Lock and Edit**.
- c. Select the Managed Server that you want to clone (for example, **WLS_OIM1** or **WLS_SOA1**).
- d. Select **Clone**.

Name the new Managed Server **WLS_OIM n** or **WLS_SOA n** , where n is a number to identify the new Managed Server.

The rest of the steps assume that you are adding a new server to OIMHOST1, which is already running WLS_SOA1 and WLS_OIM1.

2. For the listen address, assign the host name or IP address to use for this new Managed Server. If you are planning to use server migration as recommended for this server, this should be the VIP (also called a floating IP) to enable it to move to another node. The VIP should be different from the one used by the Managed Server that is already running.
3. Create JMS Servers for SOA, Oracle Identity Manager, UMS, and BPM on the new Managed Server.
 - a. Use the Oracle WebLogic Server Administration Console to create a new persistent store for the new SOAJMS Server and name it, for example, **SOAJMSFileStore_ N** . Specify the path for the store. This should be a directory on shared storage, as recommended in [Section 4.4.4, "Directory Structure."](#)

Note: This directory must exist before the Managed Server is started or the start operation fails.

ORACLE_BASE/admin/domain_name/cluster_name/jms/SOAJMSFileStore_N

- b. Create a new JMS server for SOA, for example, *SOAJMSServer_auto_N*. Use the *SOAJMSFileStore_N* for this JMSServer. Target the *SOAJMSServer_auto_N* server to the recently created Managed Server (*WLS_SOAn*).
- c. Create a new JMS server for BPM, for example, *BPMJMSServer_auto_N*. Use the *BPMJMSServer_auto_N* for this JMSServer. Target the *BPMJMSServer_auto_N* server to the recently created Managed Server *WLS_SOAn*.
- d. Create a new persistence store for the new *BPMJMSServer* for example, *BPMJMSFileStore_N*. Specify the path for the store. This should be a directory on shared storage, as recommended in [Section 4.4.4, "Directory Structure."](#)
- e. Create a new persistence store for the new *UMSJMServer*, for example, *UMSJMSFileStore_N*. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 4.4.4, "Directory Structure."](#)

ORACLE_BASE/admin/domain_name/cluster_name/jms/UMSJMSFileStore_N.

Note: This directory must exist before the Managed Server is started or the start operation fails. You can also assign *SOAJMSFileStore_N* as store for the new UMS JMS servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

- f. Create a new JMS Server for UMS, for example, *UMSJMSServer_N*. Use the *UMSJMSFileStore_N* for this JMSServer. Target the *UMSJMSServer_N* server to the recently created Managed Server (*WLS_SOAn*).
- g. Create a new persistence store for the new *OIMJMSServer*, for example, *OIMJMSFileStore_N*. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 4.4.4, "Directory Structure."](#)

ORACLE_BASE/admin/domain_name/cluster_name/jms/OIMJMSFileStore_N

Note: This directory must exist before the Managed Server is started or the start operation fails. You can also assign *SOAJMSFileStore_N* as store for the new Oracle Identity Manager JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.

- h. Create a new JMS Server for Oracle Identity Manager, for example, *OIMJMSServer_N*. Use the *OIMJMSFileStore_N* for this JMSServer. Target the *OIMJMSServer_N* server to the recently created Managed Server (*WLS_OIMn*).
- i. Update the SubDeployment targets for the SOA JMS Module to include the recently created SOA JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **SOAJMSModule** (represented as a hyperlink in the **Names** column of the table). The Settings page for

SOAJMSModule appears. Click the **SubDeployments** tab. The subdeployment module for **SOAJMS** appears.

Note: This subdeployment module name is a random name in the form of SOAJMSServerXXXXXX resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click the SOAJMSServerXXXXXX subdeployment. Add the new JMS Server for SOA called SOAJMSServer_N to this subdeployment. Click **Save**.

- j. Update the SubDeployment targets for the UMSJMSSystemResource to include the recently created UMS JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **UMSJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for UMSJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for UMSJMS appears.

Note: This subdeployment module name is a random name in the form of UCMJMSServerXXXXXX resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click the UMSJMSServerXXXXXX subdeployment. Add the new JMS Server for UMS called UMSJMSServer_N to this subdeployment. Click **Save**.

- k. Update the SubDeployment targets for the BPMJMSSystemResource to include the recently created BPM JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **BPMJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for BPMJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for BPMJMS appears.

Note: This subdeployment module name is a random name in the form of BPMJMSServerXXXXXX resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click the **BPMJMSServerXXXXXX** subdeployment. Add the new JMS Server for BPM called BPMJMSServer_N to this subdeployment. Click **Save**.

- l. Update the SubDeployment targets for OIMJMSModule to include the recently created Oracle Identity Manager JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **OIMJMSModule** (represented as a hyperlink in the Names column of the table). The Settings page for OIMJMSSystemResource appears. Click the **SubDeployments** tab. The subdeployment module for OIMJMS appears.

Note: This subdeployment module name is a random name in the form of `OIMJMSServerXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_OIM1` and `WLS_OIM2`).

Click the `OIMJMSServerXXXXXX` subdeployment. Add the new JMS Server for Oracle Identity Manager called `OIMJMSServer_N` to this subdeployment. Click **Save**.

4. Configure Oracle Coherence, as described in [Section 14.7, "Configuring Oracle Coherence for Deploying Composites."](#)
5. Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.

From the Administration Console, select the **Server_name** > **Services** tab. Under Default Store, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.

6. Disable host name verification for the new Managed Server. Before starting and verifying the `WLS_SOAn` Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `OIMHOSTn`. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification settings is propagated to the cloned server).

To disable host name verification:

- a. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.
- b. Expand the **Environment** node in the Domain Structure window.
- c. Click **Servers**. The Summary of Servers page appears.
- d. Select `WLS_SOAn` in the Names column of the table. The Settings page for the server appears.
- e. Click the **SSL** tab.
- f. Click **Advanced**.
- g. Set **Hostname Verification** to None.
- h. Click **Save**.
7. Repeat Steps 6a through 6h to disable host name verification for the `WLS_OIMn` Managed Servers. In Step d, select `WLS_OIMn` in the Names column of the table.
8. Click **Activate Changes** from the Change Center menu.
9. Update the SOA host and port using Oracle Enterprise Manager Fusion Middleware Control. Follow these steps:
 - a. Open a browser and go to Oracle Enterprise Manager Fusion Middleware Control at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
 - b. Log in to Oracle Enterprise Manager Fusion Middleware Control using the Admin user credentials.

Note: At least one of the Oracle Identity Manager Managed Servers must be running for when these steps are executed.

- c. Navigate to **Identity and Access**, and then **oim**.
- d. Right-click **oim** and navigate to **System MBean Browser**.
- e. Under **Application Defined MBeans**, navigate to **oracle.iam**, **Application:oim**, **XMLConfig**, **Config**, **XMLConfig.SOAConfig**, and then **SOAConfig**.
- f. Update the value for the **Rmiurl** attribute with the host and port of the new SOA server. Click **Apply** to save the changes.
- g. The **Rmiurl** attribute is used for accessing SOA EJBs deployed on SOA Managed Servers. This is the application server URL. The following is an example value for this attribute:


```
t3://soa_cluster
```
10. Restart the WebLogic Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
11. Start and test the new Managed Server from the Administration Console.
 - a. Shut down the existing Managed Servers in the cluster.
 - b. Ensure that the newly created Managed Server, **WLS_SOAn**, is up.
 - c. Access the application on the newly created Managed Server (<http://vip:port/soa-infra>). The application should be functional.
12. Configure the newly created managed server for server migration. Follow the steps in [Section 17.6, "Configuring Server Migration Targets"](#) to configure server migration.
13. Test server migration for this new server. Follow these steps from the node where you added the new server:
 - a. Stop the **WLS_SOAn** Managed Server.
To do this, run:


```
kill -9 pid
```

on the process ID (PID) of the Managed Server. You can identify the PID of the node using

```
ps -ef | grep WLS_SOAn
```
 - b. Watch the Node Manager Console. You should see a message indicating that the floating IP address for **WLS_SOAn** has been disabled.
 - c. Wait for the Node Manager to try a second restart of **WLS_SOAn**. Node Manager waits for a fence period of 30 seconds before trying this restart.
 - d. Once Node Manager restarts the server, stop it again. Now Node Manager should log a message indicating that the server will not be restarted again locally.

20.4.1.2.4 Scaling Up Oracle Identity Federation The application tier already has a node (IDMHOST2) running a Managed Server configured with Oracle Identity Federation.

The node contains a WebLogic Server home and an Oracle Fusion Middleware Identity Management home on the local disk.

The existing installations (WebLogic Server home, Oracle Fusion Middleware home, and domain directories) can be used for creating a new Managed Server for Oracle Identity Federation.

1. Follow the steps in [Section 15.5, "Configuring Oracle Identity Federation on IDMHOST2"](#) to scale up the topology for Oracle Identity Federation.
2. Be sure to choose a port other than 7499, which is already in use.
3. Follow the steps in [Section 15.6, "Provisioning the Managed Servers on the Local Disk"](#) to provision the new Oracle Identity Federation managed server on the local disk.
4. Reconfigure the Oracle HTTP Server module with the new Managed Server. Follow the instructions in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment,"](#) to complete this task.

20.4.1.3 Scaling Up the Web Tier

The web tier already has a node running an instance of the Oracle HTTP Server. The existing Oracle HTTP Server binaries can be used for creating the new Oracle HTTP Server instance. To scale up the Oracle HTTP Server, follow the steps in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment."](#)

1. Use the Oracle Fusion Middleware 11g Web Tier Utilities Configuration Wizard to scale up the topology, as described in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment."](#)
2. Copy all files created in `ORACLE_INSTANCE/config/OHS/component/moduleconf` from the existing web tier configuration to the new one.
3. Register the new Oracle HTTP Server instance, as described in [Section 8.8.4, "Registering Oracle HTTP Server with WebLogic Server."](#)
4. Reconfigure the load balancer with the host and port information of the new Oracle HTTP Server instance.

20.4.2 Scaling Out the Topology

In scaling out a topology, new servers are added to new nodes. The components in all three tiers of the Oracle Identity Management topology described in this manual can be scaled out by adding a new server instance to a new node.

This section contains the following topics:

- [Section 20.4.2.1, "Scaling Out the Directory Tier"](#)
- [Section 20.4.2.2, "Scaling Out the Application Tier"](#)
- [Section 20.4.2.3, "Scaling Out the Web Tier"](#)

20.4.2.1 Scaling Out the Directory Tier

The directory tier consists of the two Oracle Internet Directory nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Internet Directory instance and the two Oracle Virtual Directory nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Virtual Directory instance. The Oracle Internet Directory or Oracle Virtual Directory instances can be scaled out by adding new nodes to the directory tier.

20.4.2.1.1 Scaling Out Oracle Internet Directory The directory tier has two Oracle Internet Directory nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Internet Directory instance. The Oracle Internet Directory instances can be scaled out by adding a new node to the existing Oracle Internet Directory cluster. To scale out Oracle Internet Directory instances, follow these steps:

1. Follow the steps in [Section 9.4.2, "Configuring an Additional Oracle Internet Directory Instance"](#) to add a new node running Oracle Internet Directory.
2. Follow the steps in [Section 9.5.1, "Registering Oracle Internet Directory with the WebLogic Server Domain \(IDMDomain\)"](#) to register the new Oracle Internet Directory instance with the WebLogic domain.
3. Configure SSL server authentication mode for the new instance, as described in [Section 9.5.3, "Configuring Oracle Internet Directory to Accept Server Authentication Mode SSL Connections."](#)
4. Reconfigure the load balancer with the host and port information of the new Oracle Internet Directory instance.

20.4.2.1.2 Scaling Out Oracle Virtual Directory The directory tier has two nodes (LDAPHOST1 and LDAPHOST2), each running an Oracle Virtual Directory instance. Oracle Virtual Directory can be scaled out by adding a new node configured to run Oracle Virtual Directory to the directory tier. To scale out Oracle Virtual Directory instances, follow these steps:

1. Follow the steps in [Section 12.3.2, "Configuring an Additional Oracle Virtual Directory"](#) to add a new node running Oracle Virtual Directory.
2. Follow the steps in these sections to register the new Oracle Virtual Directory instance with the WebLogic domain.
 - [Section 12.4, "Post-Configuration Steps"](#)
 - [Section 12.6, "Validating the Oracle Virtual Directory Instances"](#)
 - [Section 12.7, "Creating ODSM Connections to Oracle Virtual Directory"](#)
 - [Section 12.8, "Creating Adapters in Oracle Virtual Directory"](#)
3. Reconfigure the load balancer with the host and port information of the new Oracle Virtual Directory instance.

20.4.2.2 Scaling Out the Application Tier

The application tier has two nodes (IDMHOST1 and IDMHOST2) running Managed Servers for Oracle Access Manager, Oracle Identity Federation and Oracle Directory Services Manager, and two nodes (OIMHOST1 and OIMHOST2) running the Oracle Identity Manager.

Some of the procedures described in this section show you how to create a new WebLogic managed server. If you add a new managed server to your topology, after adding the managed server you must update your Oracle HTTP Server configuration files (on all nodes) and add the new server to the existing WebLogic cluster directives.

For example if you add a new Oracle Access Manager server, you must update `sso_vh.conf` to include the new managed server.

Update `sso_vh.conf` as follows:

```
<Location /oam>
SetHandler weblogic-handler
WebLogicCluster
```

```
IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100, IDMHOST3.mycompany.com:14100
</Location>
```

Once you have updated `sso_vh.conf`, restart the Oracle HTTP server(s) as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#) Oracle recommends that you do this sequentially to prevent loss of service.

20.4.2.2.1 Scaling Out Oracle Identity Federation The application tier has two nodes (IDMHOST1 and IDMHOST2) running a Managed Server configured with Oracle Identity Federation. The Oracle Identity Federation instances can be scaled out by adding a new node with a Managed Server to the existing cluster.

Use the existing installations in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

To scale out the Oracle Identity Federation instances, follow these steps:

1. Follow the steps in these sections to scale out the Oracle Identity Federation instances in the topology.
 - [Section 15.5, "Configuring Oracle Identity Federation on IDMHOST2"](#)
 - [Section 15.6, "Provisioning the Managed Servers on the Local Disk"](#)
 - [Section 15.7, "Validating Oracle Identity Federation"](#)
 - [Section 15.8, "Configure the Enterprise Manager Agents"](#)
2. Follow the steps in [Section 15.10, "Configuring Oracle Identity Federation to work with the Oracle Web Tier"](#) to add the newly added Managed Server host name and port to the list WebLogicCluster parameter.

20.4.2.2.2 Scaling Out ODSM The application tier has two nodes (IDMHOST1 and IDMHOST2) running a Managed Server configured with Oracle Directory Services Manager. The Oracle Directory Services Manager instances can be scaled out by adding a new node with a Managed Server to the existing cluster.

Use the existing installations in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

To scale out ODSM instances, follow these steps:

1. Follow the steps in [Section 10.4, "Expanding the ODSM Cluster"](#) to scale out Oracle Directory Services Manager instances in the topology.
2. Reconfigure the Oracle HTTP Server module with the new Managed Server.
Follow the steps in [Section 10.6, "Configuring ODSM to work with the Oracle Web Tier"](#) for the instructions to complete this task.
Add the newly added Managed Server host name and port to the list WebLogicCluster Parameter.

20.4.2.2.3 Scaling Out Oracle Access Manager 11g Scale out is very similar to scale up but first requires the software to be installed on the new node.

Use the existing installations in shared storage for creating the new Managed Servers. You do not need to install WebLogic Server or Identity Management binaries in a new

location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

Note: If you are using shared storage, allow the new host access to that shared storage area.

1. On the new node, mount the existing Middleware home, which should include the SOA installation and the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain.
2. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the `MW_HOME/bea/beahomelist` file and add `ORACLE_BASE/product/fmw` to it.
3. Log in to the Oracle WebLogic Server Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
4. From the Domain Structure window of the Oracle WebLogic Server Administration Console, expand the **Environment** node and then **Servers**. The Summary of Servers page appears.
5. Click **Lock & Edit** from the Change Center menu.
6. Select an existing server on the host you want to extend, for example: **WLS_OAM1**.
7. Click **Clone**.
8. Enter the following information:
 - **Server Name:** A new name for the server, for example: **WLS_OAM3**.
 - **Server Listen Address:** The name of the host on which the Managed Server runs.
 - **Server Listen Port:** The port the new Managed Server uses. This port must be unique within the host.
9. Click **OK**.
10. Click the newly created server **WLS_OAM3**.
11. Set the SSL listen port. This should be unique on the host that the Managed Server runs on.
12. Click **Save**.
13. Disable host name verification for the new Managed Server. Before starting and verifying the **WLS_OAM3** Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in `IDMHOSTn`.

If the source server from which the new one was cloned had already disabled host name verification, these steps are not required, as the host name verification settings was propagated to the cloned server. To disable host name verification, proceed as follows:

- a. In Oracle Enterprise Manager Fusion Middleware Control, select Oracle WebLogic Server Administration Console.
- b. Expand the **Environment** node in the Domain Structure pane.

- c. Click **Servers**. The Summary of Servers page appears.
 - d. Select **WLS_OAM3** in the Names column of the table. The Settings page for server appears.
 - e. Click the **SSL** tab.
 - f. Click **Advanced**.
 - g. Set **Hostname Verification** to **None**.
 - h. Click **Save**.
14. Click **Activate Configuration** from the Change Center menu.
 15. Restart the WebLogic Administration Server as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
 16. Pack the domain on IDMHOST1 using the command:

```
pack.sh -domain=ORACLE_BASE/admin/IDMDomain/aserver/IDMDomain -template
=/tmp/IDMDomain.jar -template_name="OAM Domain" -managed=true
```

The `pack.sh` script is located in `MW_HOME/oracle_common/common/bin`.

17. Unpack the domain on the new host using the command:

```
unpack.sh -domain=ORACLE_BASE/admin/IDMDomain/msserver/IDMDomain
-template=/tmp/IDMDomain.jar -app_dir=ORACLE_
BASE/admin/IDMDomain/msserver/applications
```

The `unpack.sh` script is located in `MW_HOME/oracle_common/common/bin`.

18. Start Node Manager and update the property file.
 - a. Start and stop Node Manager as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
 - b. Run the script `setNMProps.sh`, which is located in `ORACLE_COMMON_HOME/common/bin`, to update the node manager properties file, for example:

```
cd ORACLE_COMMON_HOME/common/bin
./setNMProps.sh
```
 - c. Start Node Manager once again as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

Register the new Managed Server with Oracle Access Manager. The new Managed Server now must be configured as an Oracle Access Manager server. You do this from the Oracle OAM console, as follows:

1. Log in to the OAM console as the `oamadmin` user. Use the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
2. Click the **System Configuration** tab.
3. Click **Server Instances**.
4. Select **Create** from the Actions menu.
5. Enter the following information:
 - **Server Name:** `WLS_OAM3`
 - **Host:** Host that the server is running on, `IDMHOST3`.
 - **Port:** Listen port that was assigned when the Managed Server was created.

- **OAM Proxy Port:** Port you want the Oracle Access Manager proxy to run on. This is unique for the host.
- **Proxy Server ID:** `AccessServerConfigProxy`
- **Mode:** Set to `Open` or `Simple`, depending on the mode your existing Oracle Access Manager servers are operating in.

6. Click `Apply`.

Add the newly created Oracle Access Manager server to all WebGate profiles that might be using it, such as `Webgate_IDM` and `IAMSuiteAgent`.

For example, to add the Oracle Access Manager server to `Webgate_IDM`, access the OAM console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#) Then proceed as follows:

1. Log in as the Oracle Access Manager admin user you created in [Section 11.5, "Preparing the Identity Store."](#)
2. Click the **System Configuration** tab.
3. Expand **Access Manager Settings - SSO Agents - OAM Agents**.
4. Click the open folder icon, then click **Search**.
You should see the WebGate agent **Webgate_IDM**.
5. Click the agent **Webgate_IDM**.
6. Select **Edit** from the **Actions** menu.
7. Click **+** in the **Primary Server** list (or the secondary server list if this is a secondary server).
8. Select the newly created managed server from the **Server** drop down list.
9. Set **Max Connections** to 4.
10. Click **Apply**

Repeat Steps 5 through 10 for `IAMSuiteAgent` and other WebGates that are in use.

Update the Web Tier. Now that the new Managed Server has been created and started, the web tier starts to direct requests to it. Best practice, however, is to inform the web server that the new Managed Server has been created.

You do this by updating the file `sso_vh.conf` on each of the web tiers. This file resides in the directory: `ORACLE_INSTANCE/config/OHS/component name/moduleconf`.

Add the new server to the `WebLogicCluster` directive in the file, for example, change:

```
<Location /oam>
  SetHandler weblogic-handler
  WebLogicCluster IDMH0ST1.mycompany.com:14100,IDMH0ST2.mycompany.com:14100
</Location>
```

```
<Location /fusion_apps>
  SetHandler weblogic-handler
  WebLogicCluster IDMH0ST1.mycompany.com:14100,IDMH0ST2.mycompany.com:14100
</Location>
```

to:

```
<Location /oam>
```

```
SetHandler weblogic-handler
WebLogicCluster
IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100, IDMHOST3.mycompany.com:14100
</Location>

<Location /fusion_apps>
SetHandler weblogic-handler
WebLogicCluster
IDMHOST1.mycompany.com:14100, IDMHOST2.mycompany.com:14100, IDMHOST3.mycompany.com:14100
</Location>
```

20.4.2.2.4 Scaling Out Oracle Identity Manager (Adding Managed Servers to New Nodes) When you scale out the topology, you add new Managed Servers configured with OIM and SOA to new nodes.

Before performing the steps in this section, check that you meet these requirements:

- There must be existing nodes running Managed Servers configured with OIM and SOA within the topology.
- The new node can access the existing home directories for WebLogic Server, OIM, and SOA.

Use the existing installations in shared storage for creating a new WLS_SOA or WLS_OIM Managed Server. You do not need to install WebLogic Server, OIM, or SOA binaries in a new location but you do need to run pack and unpack to bootstrap the domain configuration in the new node.

Notes:

- If there is no existing installation in shared storage, installing WebLogic Server, IAM, and SOA in the new nodes is required as described in [Section 14.7, "Configuring Oracle Coherence for Deploying Composites."](#)
 - When an *ORACLE_HOME* or *WL_HOME* is shared by multiple servers in different nodes, Oracle recommends keeping the Oracle Inventory and Middleware home list in those nodes updated for consistency in the installations and application of patches. To update the oraInventory in a node and attach an installation in a shared storage to it, use:


```
ORACLE_HOME/oui/bin/attachHome.sh
```
 - To update the Middleware home list to add or remove a *WL_HOME*, edit the *user_home/boa/beahomelist* file. See the following steps.
-

Follow these steps for scaling out the topology:

1. On the new node, mount the existing Middleware home, which should include the Oracle Fusion Middleware installation and the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain.
2. To attach *IAM_HOME* in shared storage to the local Oracle Inventory, execute the following command:

```
cd ORACLE_BASE/product/fmw/iam/oui/bin
```

```
/attachHome.sh -jreLoc JAVA_HOME
```

3. To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the `MW_HOME/bea/beahomelist` file and add `ORACLE_BASE/product/fmw` to it.
4. Log in to the Oracle WebLogic Administration Console at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
5. Create a new machine for the new node to be used, and add the machine to the domain.
6. Update the machine's Node Manager's address to map the IP address of the node that is being used for scale out.
7. Use the Oracle WebLogic Server Administration Console to clone the managed servers `WLS_OIM` and `WLS_SOA1` into new Managed Servers. Name them `WLS_SOA n` and `WLS_OIM n` , respectively, where n is a number.

Note: These steps assume that you are adding a new server to node n , where no Managed Server was running previously.

8. Assign the host names or IP addresses to the listen addresses of the new Managed Servers.
9. If you are planning to use server migration for this server (which Oracle recommends) this should be the VIP address (also called a floating IP address) for the server. This VIP address should be different from the one used for the existing Managed Server.
10. Create JMS servers for SOA, Oracle Identity Manager (if applicable), and UMS on the new Managed Server.
 - a. Use the Oracle WebLogic Server Administration Console to create a new persistent store for the new SOAJMS Server and name it, for example, `SOAJMSFileStore_ N` . Specify the path for the store. This should be a directory on shared storage as recommended in [Section 4.4.4, "Directory Structure."](#) For example:

```
ORACLE_BASE/admin/domain_name/cluster_
name/jms/SOAJMSFileStore_ $N$ 
```

Note: This directory must exist before the Managed Server is started or the start operation fails.

- b. Create a new JMS Server for SOA, for example, `SOAJMS Server_auto_ N` . Use the `SOAJMSFileStore_ N` for this JMSServer. Target the `SOAJMS Server_auto_ N` Server to the recently created Managed Server (`WLS_SOA n`).
- c. Create a new persistence store for the new UMSJMSServer, and name it, for example, `UMSJMSFileStore_ N` . Specify the path for the store. This should be a directory on shared storage as recommended in [Section 4.4.4, "Directory Structure."](#)

```
ORACLE_BASE/admin/domain_name/cluster_
name/jms/UMSJMSFileStore_ $N$ 
```

Notes:

- This directory must exist before the Managed Server is started or the start operation fails.
 - It is also possible to assign `SOAJMSFileStore_N` as the store for the new UMS JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.
-

- d. Create a new JMS server for UMS: for example, `UMSJMSServer_N`. Use the `UMSJMSFileStore_N` for this JMS server. Target the `UMSJMSServer_N` server to the recently created Managed Server (`WLS_SOAn`).
- e. Create a new persistence store for the new `BPMJMSServer`, and name it, for example, `BPMJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 4.4.4, "Directory Structure."](#)

```
ORACLE_BASE/admin/domain_name/cluster_
name/jms/BPMJMSFileStore_N
```

Notes:

- This directory must exist before the Managed Server is started. Otherwise, the start operation fails.
 - It is also possible to assign `SOAJMSFileStore_N` as the store for the new BPM JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.
-

- f. Create a new JMS server for BPM, for example, `BPMJMSServer_N`. Use the `BPMJMSFileStore_N` for this JMS server. Target the `BPMJMSServer_N` server to the recently created Managed Server (`WLS_SOAn`).
- g. Create a new persistence store for the new `OIMJMSServer`, and name it, for example, `OIMJMSFileStore_N`. Specify the path for the store. This should be a directory on shared storage as recommended in [Section 4.4.4, "Directory Structure."](#)

```
ORACLE_BASE/admin/domain_name/cluster_name/jms/OIMJMSFileStore_N
```

Notes:

- This directory must exist before the Managed Server is started or the start operation fails.
 - It is also possible to assign `SOAJMSFileStore_N` as the store for the new Oracle Identity Manager JMS Servers. For the purpose of clarity and isolation, individual persistent stores are used in the following steps.
-

- h. Create a new JMS Server for Oracle Identity Manager: for example, `OIMJMSServer_N`. Use the `OIMJMSFileStore_N` for this JMS Server. Target

the `OIMJMSServer_N` Server to the recently created Managed Server (`WLS_OIMn`).

- i. Update the SubDeployment targets for the `BPMJMSSystemResource` to include the recently created BPM JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **BPMJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for `BPMJMSSystemResource` appears. Click the **SubDeployments** tab. The subdeployment module for BPMJMS appears.

Note: This subdeployment module name is a random name in the form of `BPMJMSServerXXXXXX` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `BPMJMSServerXXXXXX` subdeployment. Add the new JMS Server for BPM called `BPMJMSServer_N` to this subdeployment. Click **Save**.

- j. Update the SubDeployment targets for the SOA JMS Module to include the recently created SOA JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **SOAJMSModule** (represented as a hyperlink in the **Names** column of the table). The Settings page for **SOAJMSModule** appears. Open the SubDeployments tab. The subdeployment module for **SOAJMS** appears.

Note: This subdeployment module name is a random name in the form of `SOAJMSServer` resulting from the Configuration Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `SOAJMSServerXXXXXX` subdeployment. Add the new JMS Server for SOA called `SOAJMSServer_N` to this subdeployment. Click **Save**.

- k. Update the SubDeployment targets for `UMSJMSSystemResource` to include the recently created UMS JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose **JMS Modules** from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **UMSJMSSystemResource** (represented as a hyperlink in the **Names** column of the table). The Settings page for `UMSJMSSystemResource` appears. Open the **SubDeployments** tab. The subdeployment module for UMSJMS appears.

Note: This subdeployment module is a random name in the form of `UMSJMSServerXXXXXX` resulting from the Config Wizard JMS configuration for the first two servers (`WLS_SOA1` and `WLS_SOA2`).

Click the `UMSJMSServerXXXXXX` subdeployment. Add the new JMS Server for UMS called `UMSJMSServer_N` to this subdeployment. Click **Save**.

- I. Update the SubDeployment Targets for `OIMJMSModule` to include the recently created Oracle Identity Manager JMS Server. To do this, expand the **Services** node and then expand the **Messaging** node. Choose JMS Modules from the Domain Structure window of the Oracle WebLogic Server Administration Console. The JMS Modules page appears. Click **OIMJMSModule** (represented as a hyperlink in the Names column of the table). The Settings page for `OIMJMSModule` appears. Click the **SubDeployments** tab. The subdeployment module for `OIMJMS` appears.

Note: This subdeployment module is a random name in the form of `OIMJMSServerXXXXXX` resulting from the Config Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click the `OIMJMSXXXXXX` subdeployment. Add the new JMS Server for Oracle Identity Manager called `OIMJMSServer_N` to this subdeployment. Click **Save**.

11. Click **Activate Configuration** from the Change Center menu.
12. Run the `pack` command to create a template pack. Run it on `IDMHOST1` if you are using a single domain or on `OIMHOST1` if you are using a split domain. Proceed as follows:

```
cd ORACLE_COMMON_HOME/common/bin
./pack.sh -managed=true -domain=/u01/app/oracle/admin/domain_
name/aserver/domain_name -template=/u01/app/oracle/admin/templates/oim_
domain.jar -template_name="OIM Domain"
```

Run the `scp` command on `IDMHOST1` or `OIMHOST1` to copy the template file created to `IDMHOSTN` or `OIMHOSTN`. For example:

```
scp ORACLE_BASE/admin/templates/oim_domain.jar OIMHOSTN:ORACLE_
BASE/admin/templates/oim_domain.jar
```

Run the `unpack` command on `IDMHOSTN` or `OIMHOSTN` to unpack the template in the Managed Server domain directory as follows:

```
cd ORACLE_BASE/product/fmw/soa/common/bin
./unpack.sh -domain=ORACLE_BASE/admin/domain_name/mserver/domain_name
-template=ORACLE_BASE/admin/templates/oim_domain.jar -app_dir=ORACLE_
BASE/admin/domain_name/mserver/applications
```

13. Configure Oracle Coherence, as described in [Section 14.7, "Configuring Oracle Coherence for Deploying Composites."](#)
14. Update the SOA host and port using Oracle Enterprise Manager Fusion Middleware Control. Follow these steps:
 - a. Open a browser and go to Oracle Enterprise Manager Fusion Middleware Control at the URL listed in [Section 20.2, "About Identity Management Console URLs."](#)
 - b. Log in to Oracle Enterprise Manager Fusion Middleware Control using the admin user credentials.

Note: At least one of the Oracle Identity Manager Managed Servers must be running for when these steps are executed.

- c. Navigate to **Identity and Access**, and then **oim**.
- d. Right-click **oim** and navigate to **System MBean Browser**.
- e. Under **Application Defined MBeans**, navigate to **oracle.iam**, **Application:oim**, **XMLConfig**, **Config**, **XMLConfig.SOAConfig**, and then **SOAConfig**.
- f. Update the value for the **Rmiurl** attribute with the host and port of the new SOA server. Click **Apply** to save the changes.
- g. The **Rmiurl** attribute is used for accessing SOA EJBs deployed on SOA Managed Servers. This is the application server URL. The following is an example value for this attribute:

```
t3://soa_cluster
```

15. Configure TX persistent store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage.

From the Administration Console, select **Server_name** > **Services** tab. Under **Default Store**, in **Directory**, enter the path to the folder where you want the default persistent store to store its data files.

16. Disable host name verification for the new Managed Server. Before starting and verifying the WLS_SOAn and WLS_OIMn Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for the communication between the Oracle WebLogic Administration Server and the Node Manager in OIMHOSTn. If the source server from which the new one has been cloned had already disabled host name verification, these steps are not required (the host name verification setting is propagated to the cloned server).

To disable host name verification for WLS_SOAn:

- a. Expand the **Environment** node in the **Domain Structure** window.
- b. In the Oracle Enterprise Manager Console, select **Oracle WebLogic Server Administration Console**.
- c. Click **Servers**. The Summary of Servers page appears.
- d. Select **WLS_SOAn** in the **Names** column of the table.
The Settings page for server appears.
- e. Click the **SSL** tab.
- f. Click **Advanced**.
- g. Set **Hostname Verification** to **None**.
- h. Click **Save**.

To disable host name verification for WLS_OIMn, repeat the same steps, but select **WLS_OIMn** in the **Names** column in Step d.

17. Click **Activate Configuration** from the Change Center menu.
18. Start the Node Manager on the new node. To start the Node Manager, use the installation in shared storage from the existing nodes, and start Node Manager by passing the host name of the new node as a parameter as follows:

```
WL_HOME/server/bin/startNodeManager new_node_ip
```

19. Start and test the new Managed Server from the Oracle WebLogic Server Administration Console:
 - a. Shut down all the existing Managed Servers in the cluster.
 - b. Ensure that the newly created Managed Servers, WLS_SOAn and WLS_SOAn, are running.
 - c. Access the applications on the newly created Managed Servers (<http://vip:port/soa-infra> and <http://vip:port/oim>). The applications should be functional.
20. Configure server migration for the new Managed Server.

Note: Since this new node is using an existing shared storage installation, the node is already using a Node Manager and an environment configured for server migration that includes netmask, interface, `wlsifconfig` script superuser privileges. The floating IP addresses for the new Managed Servers are already present in the new node.

Configure server migration following these steps:

- a. Log in to the Administration Console.
- b. In the left pane, expand **Environment** and select **Servers**.
- c. Select the server (represented as hyperlink) for which you want to configure migration from the **Names** column of the table. The Setting page for that server appears.
- d. Click the **Migration** tab.
- e. In the **Available** field, in the **Migration Configuration** section, select the machines to which to enable migration and click the right arrow.

Note: Specify the least-loaded machine as the migration target for the new server. The required capacity planning must be completed so that this node has enough available resources to sustain an additional Managed Server.

- f. Select the **Automatic Server Migration Enabled** option. This enables the Node Manager to start a failed server on the target node automatically.
- g. Click **Save**.
- h. Restart the Administration Server, Managed Servers, and Node Manager.
- i. Test server migration for the new servers WLS_SOAn and WLS_OIMn, as follows.

1. Determine the PID of the WLS_SOAn Managed Server by typing

```
ps -ef | grep WLS_SOAn
```

2. From the node where you added the new server, abruptly stop the WLS_SOAn Managed Server by typing:

```
kill -9 pid
```

3. Watch the Node Manager Console. You should see a message indicating that floating IP address for WLS_SOA1 has been disabled.
4. Wait for the Node Manager to try a second restart of WLS_SOA n . Node Manager waits for a fence period of 30 seconds before trying this restart.
5. Once Node Manager restarts the server, stop it again. Now Node Manager should log a message indicating that the server will not be restarted again locally.
6. Repeat Steps 1-5 for WLS_OIM n .

20.4.2.3 Scaling Out the Web Tier

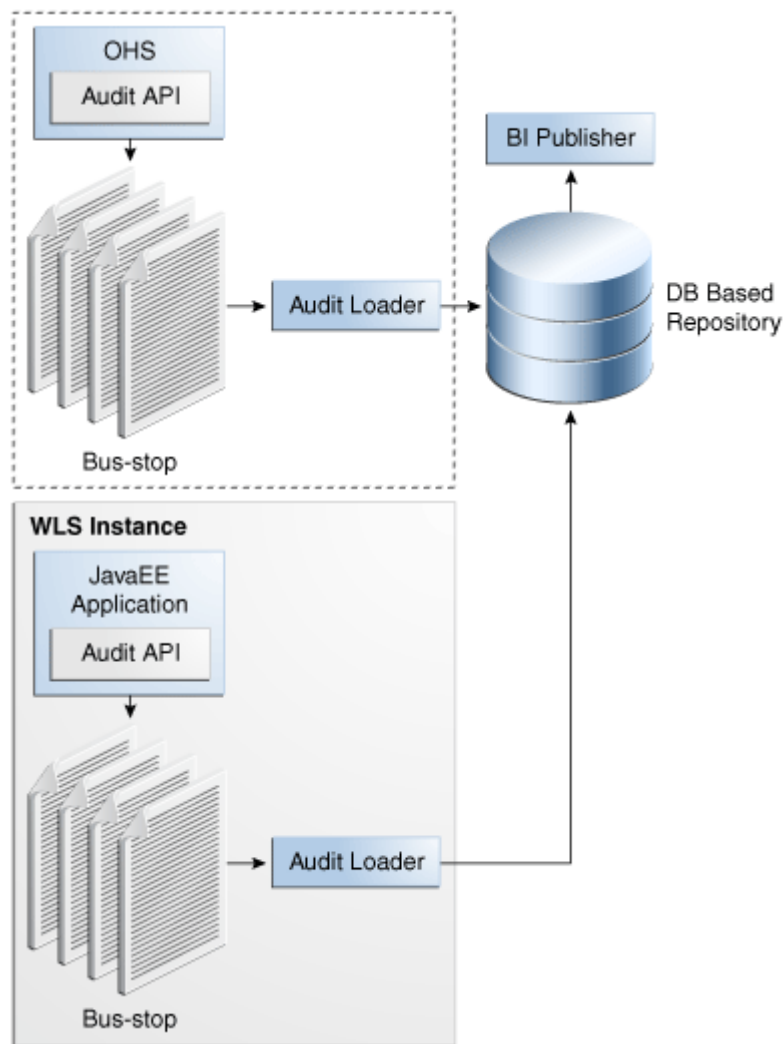
The web tier has two nodes each running an instance of the Oracle HTTP Server. The Oracle HTTP Server components can be scaled out by adding a new node configured to run Oracle HTTP Server to the web tier. To scale out Oracle HTTP Server, proceed as follows:

1. Follow the steps in [Section 6.2, "Installing Oracle HTTP Server."](#) Alternatively, on the new node, mount the existing Middleware home, if you are using shared storage.
2. Follow the steps in [Chapter 7, "Configuring the Web Tier for an Enterprise Deployment."](#)
3. Copy all files created in `ORACLE_INSTANCE/config/OHS/component/moduleconf` from the existing web tier configuration to the new one.
4. If you have enabled Single Sign-on in the topology, you must update the WebTier configuration for Single Sign-on as described in [Section 19.7, "Installing and Configuring WebGate 11g."](#)
5. Register the new Oracle HTTP Server instance as described in [Section 8.8.4, "Registering Oracle HTTP Server with WebLogic Server."](#)
6. Reconfigure the load balancer with the host and port information of the new Oracle HTTP Server instance.

20.5 Auditing Identity Management

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11g, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications are able to create application-specific audit events. For non-JavaEE Oracle components in the middleware such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications.

[Figure 20–1](#) is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework.

Figure 20–1 Audit Event Flow

The Oracle Fusion Middleware Audit Framework consists of the following key components:

- Audit APIs

These are APIs provided by the audit framework for any audit-aware components integrating with the Oracle Fusion Middleware Audit Framework. During run-time, applications may call these APIs where appropriate to audit the necessary information about a particular event happening in the application code. The interface enables applications to specify event details such as username and other attributes needed to provide the context of the event being audited.

- Audit Events and Configuration

The Oracle Fusion Middleware Audit Framework provides a set of generic events for convenient mapping to application audit events. Some of these include common events such as authentication. The framework also enables applications to define application-specific events.

These event definitions and configurations are implemented as part of the audit service in Oracle Platform Security Services. Configurations can be updated through Enterprise Manager (UI) and WLST (command-line tool).

- The Audit Bus-stop

Bus-stops are local files containing audit data before they are pushed to the audit repository. In the event where no database repository is configured, these bus-stop files can be used as a file-based audit repository. The bus-stop files are simple text files that can be queried easily to look up specific audit events. When a DB-based repository is in place, the bus-stop acts as an intermediary between the component and the audit repository. The local files are periodically uploaded to the audit repository based on a configurable time interval.

- Audit Loader

As the name implies, audit loader loads the files from the audit bus-stop into the audit repository. In the case of platform and JavaEE application audit, the audit loader is started as part of the JavaEE container start-up. In the case of system components, the audit loader is a periodically spawned process.

- Audit Repository

Audit Repository contains a pre-defined Oracle Fusion Middleware Audit Framework schema, created by Repository Creation Utility (RCU). Once configured, all the audit loaders are aware of the repository and upload data to it periodically. The audit data in the audit repository is expected to be cumulative and grow over time. Ideally, this should not be an operational database used by any other applications - rather, it should be a standalone RDBMS used for audit purposes only. In a highly available configuration, Oracle recommends that you use an Oracle Real Application Clusters (Oracle RAC) database as the audit data store.

- Oracle Business Intelligence Publisher

The data in the audit repository is exposed through pre-defined reports in Oracle Business Intelligence Publisher. The reports enable users to drill down the audit data based on various criteria. For example:

- Username
- Time Range
- Application Type
- Execution Context Identifier (ECID)

For more introductory information for the Oracle Fusion Middleware Audit Framework, see the "Introduction to Oracle Fusion Middleware Audit Framework" chapter in the *Oracle Fusion Middleware Application Security Guide*.

For information on how to configure the repository for Oracle Fusion Middleware Audit Framework, see the "Configuring and Managing Auditing" chapter in the *Oracle Fusion Middleware Application Security Guide*.

The EDG topology does not include Oracle Fusion Middleware Audit Framework configuration. The ability to generate audit data to the bus-stop files and the configuration of the audit loader are available once the products are installed. The main consideration is the audit database repository where the audit data is stored. Because of the volume and the historical nature of the audit data, it is strongly recommended that customers use a separate database from the operational store or stores being used for other middleware components.

20.6 Performing Backups and Recoveries

Table 20–2 shows the static artifacts to back up in the 11g Oracle Identity Management enterprise deployment.

Table 20–2 Static Artifacts to Back Up in the Identity Management Enterprise Deployment

Type	Host	Location	Tier
Oracle Home (database)	Oracle RAC database hosts: OIDDDBHOST1 OIDDDBHOST2	User Defined	Directory Tier
<i>MW_HOME</i> (OID)	LDAPHOST1 LDAPHOST2	Middleware home, <i>MW_HOME</i> : /u01/app/oracle/product/fmw Identity Management Oracle home, <i>IDM_ORACLE_HOME</i> : /u01/app/oracle/product/fmw/idm on both LDAPHOST1 and LDAPHOST2	Directory Tier
<i>MW_HOME</i> (OVD)	LDAPHOST1 LDAPHOST2	Middleware home, <i>MW_HOME</i> : /u01/app/oracle/product/fmw Identity Management Oracle home, <i>IDM_ORACLE_HOME</i> : /u01/app/oracle/product/fmw/idm on both LDAPHOST1 and LDAPHOST2	Directory Tier
<i>MW_HOME</i> (ODSM, OIM, OAM11g, OIF and Admin Server)	IDMHOST1 IDMHOST2	Middleware Oracle home, <i>MW_HOME</i> : /u01/app/oracle/product/fmw (Identity Management Oracle home ODSM, <i>IDM_ORACLE_HOME</i> : /u01/app/oracle/product/fmw/idm on both IDMHOST1 and IDMHOST2 (Admin server Oracle home, <i>IAM_ORACLE_HOME</i> : /u01/app/oracle/product/fmw/iam on both IDMHOST1 and IDMHOST2	Application Tier
<i>MW_HOME</i> (OHS)	WEBHOST1 WEBHOST2	Middleware Oracle home, <i>MW_HOME</i> : /u01/app/oracle/product/fmw Web Oracle Home, <i>WEB_ORACLE_HOME</i> : /u01/app/oracle/product/fmw/web on WEBHOST1 Web Oracle Home, <i>WEB_ORACLE_HOME</i> : /u01/app/oracle/product/fmw/web on WEBHOST2	Web Tier
Install Related Files	Each host	OraInventory: <i>ORACLE_BASE</i> /orainventory /etc/oratab, /etc/oraInst.loc <i>user_home</i> /bea/beahomelist (on hosts where WebLogic Server is installed) Windows registry: (<i>HKEY_LOCAL_MACHINE</i> /Oracle)	Not applicable.

Table 20–3 shows the run-time artifacts to back up in the 11g Oracle Identity Management enterprise deployment:

Table 20–3 Run-Time Artifacts to Back Up in the Identity Management Enterprise Deployments

Type	Host	Location	Tier
Domain Home	IDMHOST1 IDMHOST2	<i>ORACLE_BASE</i> /admin/ <i>IDMDomain</i> /aserver on both IDMHOST1 and IDMHOST2	Application Tier
Application Artifacts (ear and war files)	IDMHOST1 IDMHOST2	Look at all the deployments, including Oracle Directory Services Manager, through the WebLogic Server Administration Console to identify all the application artifacts.	Application Tier
OID Instance Home	LDAPHOST1 LDAPHOST2	OID Instance Home on LDAPHOST1: <i>ORACLE_BASE</i> /admin/oid1 OID Instance Home on LDAPHOST2: <i>ORACLE_BASE</i> /admin/oid2	Directory Tier
OVD Instance Home	LDAPHOST1 LDAPHOST2	OVD Instance Home on LDAPHOST1: <i>ORACLE_BASE</i> /admin/ovd1 OVD Instance Home on LDAPHOST2: <i>ORACLE_BASE</i> /admin/ovd2	Directory Tier
Oracle RAC Databases	OIDDDBHOST1 OIDDDBHOST2	User defined	Directory Tier
OAM	OAMHOST1 OAMHOST2	All the configurations are within the respective home directories described in this table. There are no instance homes.	Application Tier

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

20.7 Patching Enterprise Deployments

This section describes how to apply an Oracle Fusion Middleware patch file and how to patch Oracle Identity Management components with minimal down time.

This section contains the following topics:

- [Section 20.7.1, "Patching an Oracle Fusion Middleware Source File"](#)
- [Section 20.7.2, "Patching Identity and Access Management in a Single Domain Topology"](#)
- [Section 20.7.3, "Patching Identity and Access Management in a Split Domain Topology"](#)
- [Section 20.7.4, "Patching Identity Management Components"](#)

20.7.1 Patching an Oracle Fusion Middleware Source File

For information on patching an Oracle Fusion Middleware source file, see the *Oracle Fusion Middleware Administrator's Guide*.

20.7.2 Patching Identity and Access Management in a Single Domain Topology

In a single domain topology, apply patches as follows:

IDMDomain MW_HOME

- Common patches
- Oracle Access Manager Patches
- Oracle Identity Manager Patches
- ODSM Patches
- IDM Tool Patches

20.7.3 Patching Identity and Access Management in a Split Domain Topology

In a split domain topology where Oracle Identity Manager is located in a domain separate from other components, apply patches as follows:

IDMDomain MW_HOME

- Common patches
- Oracle Access Manager Patches
- ODSM Patches
- IDM Tool Patches

OIMDomain MW_HOME

- Common patches
- Oracle Identity Manager Patches
- IDM Tool Patches

Identity Management MW_HOME

- Common patches
- Oracle Internet Directory Patches
- Oracle Virtual Directory Patches

It is not necessary to stop processes in the IDMDomain while applying patches to the OIMDomain. Similarly, it is not necessary to stop processes in the OIMDomain while applying patches to the IDMDomain.

20.7.4 Patching Identity Management Components

To patch Oracle Identity Management components with minimal down time, it is recommended that you follow these guidelines:

1. Route the LDAP traffic from LDAPHOST1 to LDAPHOST2.
2. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (LDAPHOST1).
3. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.
4. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.
5. Test the patch.
6. Route the traffic to LDAPHOST1 again.
7. Verify the applications are working properly.

8. Route the LDAP traffic on LDAPHOST2 to LDAPHOST1.
9. Bring down the Oracle Internet Directory or Oracle Virtual Directory server on the host on which you are applying the patch (LDAPHOST2).
10. Apply the Oracle Internet Directory patch or Oracle Virtual Directory patch on the host.
11. Start the Oracle Internet Directory or Oracle Virtual Directory server on the host.
12. Test the patch.
13. Route the traffic to both hosts on which the patch has been applied (LDAPHOST1 and LDAPHOST2).

20.8 Preventing Timeouts for SQL

Most of the production deployment involves firewalls. Because database connections are made across firewalls, Oracle recommends that the firewall be configured so that the database connection is not timed out. For Oracle Real Application Clusters (Oracle RAC), the database connections are made on Oracle RAC VIPs and the database listener port. You must configure the firewall so it does not time out these connections. If such a configuration is not possible, set the `SQLNET.EXPIRE_TIME=n` parameter in the `ORACLE_HOME/network/admin/sqlnet.ora` file on the database server, where `n` is the time in minutes. Set this value to less than the known value of the timeout for the network device (that is, a firewall). For Oracle RAC, set this parameter in all of the Oracle home directories.

20.9 Troubleshooting

This section describes how to troubleshoot common issues that can arise with the Identity Management enterprise deployment described in this manual.

This section contains the following topics:

- [Section 20.9.1, "Troubleshooting Oracle Internet Directory"](#)
- [Section 20.9.2, "Troubleshooting Oracle Virtual Directory"](#)
- [Section 20.9.3, "Troubleshooting Oracle Directory Services Manager"](#)
- [Section 20.9.4, "Troubleshooting Oracle Access Manager 11g"](#)
- [Section 20.9.5, "Troubleshooting Oracle Identity Manager"](#)
- [Section 20.9.6, "Troubleshooting Oracle Identity Federation"](#)

20.9.1 Troubleshooting Oracle Internet Directory

This section describes some common problems that can arise with Oracle Internet Directory and the actions you can take to resolve the problem. It contains the following topics:

- [Section 20.9.1.1, "Oracle Internet Directory Server is Not Responsive."](#)
- [Section 20.9.1.2, "SSO/LDAP Application Connection Times Out"](#)
- [Section 20.9.1.3, "LDAP Application Receives LDAP Error 53 \(DSA Unwilling to Perform\)"](#)
- [Section 20.9.1.4, "TNSNAMES.ORA, TAF Configuration, and Related Issues"](#)

20.9.1.1 Oracle Internet Directory Server is Not Responsive.

Problem

The Oracle Internet Directory server is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Internet Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

20.9.1.2 SSO/LDAP Application Connection Times Out

Problem

The SSO/LDAP Application connection is lost to Oracle Internet Directory server

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

20.9.1.3 LDAP Application Receives LDAP Error 53 (DSA Unwilling to Perform)

Problem

The LDAP application is receiving LDAP Error 53 (DSA Unwilling to Perform). When one of the database nodes goes down during the middle of the LDAP transaction, the Oracle Internet Directory server sends error 53 to the LDAP client

Solution

To see why the Oracle Internet Directory database node went down, see the Oracle Internet Directory logs in this location:

`ORACLE_INSTANCE/diagnostics/logs/OID/oidldapd01s*.log`

20.9.1.4 TNSNAMES.ORA, TAF Configuration, and Related Issues

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

20.9.2 Troubleshooting Oracle Virtual Directory

This section describes some common problems that can arise with Oracle Virtual Directory and the actions you can take to resolve the problem. It contains the following topics:

- [Section 20.9.2.1, "Command Not Found Error When Running SSLServerConfig.sh"](#)

- [Section 20.9.2.2, "Oracle Virtual Directory is Not Responsive"](#)
- [Section 20.9.2.3, "SSO/LDAP Application Connection Times Out"](#)
- [Section 20.9.2.4, "TNSNAMES.ORA, TAF Configuration, and Related Issues"](#)
- [Section 20.9.2.5, "SSLServerConfig.sh Fails with Error"](#)

20.9.2.1 Command Not Found Error When Running SSLServerConfig.sh

Problem

You get a command not found error when you run `SSLServerConfig.sh`, for example:

```
./SSLServerConfig.sh: line 169: 20110520125611: command not found
```

Solution

Edit the file `orapki.bat` (on Windows) or `orapki.sh` (on Linux) and remove any blank lines at the end of the file. Save the file and run `SSLServerConfig.sh` again.

20.9.2.2 Oracle Virtual Directory is Not Responsive

Problem

Oracle Virtual Directory is not responsive. When the load balancing router is configured to send an ICMP message to the LDAP SSL port for monitoring, the Oracle Virtual Directory server starting SSL negotiation sometimes hangs, and thus it is required that the load balancing router not use ICMP messages for monitoring the LDAP SSL port.

Solution

Use an alternative such as TCP or the LDAP protocol itself.

Also, monitoring the LDAP non-SSL port is sufficient to detect LDAP availability.

20.9.2.3 SSO/LDAP Application Connection Times Out

Problem

The SSO/LDAP Application connection is lost to the Oracle Virtual Directory server.

Solution

Verify the load balancing router timeout and SSO/Application timeout configuration parameter. The SSO/LDAP application timeout value should be less than LBR IDLE time out.

20.9.2.4 TNSNAMES.ORA, TAF Configuration, and Related Issues

Problem

Issues involving TNSNAMES.ORA, TAF configuration, and related issues.

Solution

See the *Oracle Database High Availability Overview* manual.

20.9.2.5 SSLServerConfig.sh Fails with Error

Problem

When you run `SSLServerConfig.sh` for component OVD, sometime it fails with an error similar to this:

```
>>>Enter password for weblogic:
>>>Enter your keystore name [ovdks1.jks]:
Checking the existence of ovdks1.jks in the OVD...

>>>Failed to configure your SSL server wallet
>>>Please check /scratch/aim1/edgfa/idm/rootCA/keystores/ovd/ks_check.log for
more information
```

In the log file, you see an error message like this:

```
Problem invoking WLST - Traceback (innermost last):
File "/scratch/aim1/edgfa/idm/rootCA/keystores/ovd/ovdssl-check.py", line 8, in ?
File "<iostream>", line 182, in cd
File "<iostream>", line 1848, in raiseWLSTException
WLSTException: Error occured while performing cd : Attribute
oracle.as.ovd:type=component.listenersconfig.sslconfig,name=LDAP SSL
Endpoint,instance=ovd1,component=ovd1 not found. Use ls(a) to view the
attributes
```

Solution

The problem is intermittent. To work around the issue, re-run the script.

20.9.3 Troubleshooting Oracle Directory Services Manager

This section describes some common problems that can arise with Oracle Directory Services Manager and the actions you can take to resolve the problem. It contains the following topics:

- [Section 20.9.3.1, "ODSM Browser Window and Session Issues"](#)
- [Section 20.9.3.2, "ODSM Does not Open When Invoked from Fusion Middleware Control"](#)
- [Section 20.9.3.3, "ODSM Failover is Not Transparent"](#)
- [Section 20.9.3.4, "ODSM Loses Connection and Displays Message that LDAP Server is Down"](#)
- [Section 20.9.3.5, "ODSM Loses Connection to Instance Using ORAC Database"](#)
- [Section 20.9.3.6, "OHS Must Be Configured to Route ODSM Requests to Multiple Oracle WebLogic Servers"](#)
- [Section 20.9.3.7, "ODSM is Not Accessible"](#)

20.9.3.1 ODSM Browser Window and Session Issues

After you have logged into Oracle Directory Services Manager, you can connect to multiple directory instances from the same browser window.

Avoid using multiple windows of the same browser program to connect to different directories at the same time. Doing so can cause a Target unreachable error.

You can log in to the same Oracle Directory Services Manager instance from different browser programs, such as Internet Explorer and Firefox, and connect each to a different directory instance.

If you change the browser language setting, you must update the session to use the new setting. To update the session, either disconnect the current server connection, refresh the browser page (either reenter the Oracle Directory Services Manager URL in the URL field and press enter or press F5) and reconnect to the same server, or quit and restart the browser.

20.9.3.2 ODSM Does not Open When Invoked from Fusion Middleware Control

Problem

Oracle Directory Services Manager does not open after you attempt to invoke it from Oracle Enterprise Manager Fusion Middleware Control by selecting one of the options from the **Directory Services Manager** entry in the **Oracle Virtual Directory** menu in the Oracle Virtual Directory target or the **Oracle Internet Directory** menu in the Oracle Internet Directory target.

Solution

This is probably an installation problem. See the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management*.

20.9.3.3 ODSM Failover is Not Transparent

Problem

When you perform an Oracle Directory Services Manager failover using Oracle HTTP Server, the failover is not transparent. You see this behavior when you perform the following steps:

1. Oracle Directory Services Manager is deployed in a High Availability active-active configuration using Oracle HTTP Server.
2. Display an Oracle Directory Services Manager page using the Oracle HTTP Server name and port number.
3. Make a connection to an Oracle Internet Directory or Oracle Virtual Directory server.
4. Work with the Oracle Internet Directory or Oracle Virtual Directory server using the current Oracle Directory Services Manager Oracle HTTP Server host and port.
5. Shut down one Managed Server at a time using the WebLogic Server Administration Console.
6. Go back to the Oracle Directory Services Manager page and port, and the connection which was established earlier with Oracle Internet Directory or Oracle Virtual Directory. When you do, a message is displayed advising you to re-establish a new connection to the Oracle Directory Services Manager page.

Solution

If you encounter this problem, perform the following steps:

1. In your web browser, exit the current Oracle Directory Services Manager page.
2. Launch a new web browser page and specify the same Oracle Directory Services Manager Oracle HTTP Server name and port.
3. Re-establish a new connection to the Oracle Internet Directory or Oracle Virtual Directory server you were working with earlier.

20.9.3.4 ODSM Loses Connection and Displays Message that LDAP Server is Down

Problem

Oracle Directory Services Manager temporarily loses its connection to Oracle Internet Directory and displays the message LDAP Server is down.

Solution

In a High Availability configuration where Oracle Directory Services Manager is connected to Oracle Internet Directory through a load balancer, Oracle Directory Services Manager reports that the server is down during failover from one instance of Oracle Internet Directory to another. In other configurations, this message might indicate that Oracle Internet Directory has been shut down and restarted. In either case, the connection is reestablished in less than a minute, and you are able to continue without logging in again.

20.9.3.5 ODSM Loses Connection to Instance Using ORAC Database

Problem

Oracle Directory Services Manager temporarily loses its connection to an Oracle Internet Directory or Oracle Virtual Directory instance that is using an Oracle RAC Database. Oracle Directory Services Manager might display the message `LDAP error code 53 - Function not implemented`.

Solution

This error can occur during failover of the Oracle Database that the Oracle Internet Directory or Oracle Virtual Directory instance is using. The connection is reestablished in less than a minute, and you are able to continue without logging in again.

20.9.3.6 OHS Must Be Configured to Route ODSM Requests to Multiple Oracle WebLogic Servers

Problem

You must perform the following steps to configure Oracle HTTP Server to route Oracle Directory Services Manager requests to multiple Oracle WebLogic Servers in a clustered Oracle WebLogic Server environment.

Solution

Perform these steps:

1. Create a backup copy of the Oracle HTTP Server's `admin.conf` file, which is located in `ORACLE_INSTANCE/config`. The backup copy provides a source to revert to if you encounter problems after performing this procedure.
2. Add the following text to the end of the Oracle HTTP Server's `admin.conf` file and replace the variable placeholder values with the host names and Managed Server port numbers specific to your environment. Be sure to use the `<Location /odsm/ >` as the first line in the entry. Using `<Location /odsm/faces >` or `<Location /odsm/faces/odsm.jspx >` can distort the appearance of the Oracle Directory Services Manager interface.

```
<Location /odsm/ >
SetHandler weblogic-handler
WebLogicCluster host-name-1:managed-server-port,host-name_2:managed_server_port
</Location>
```


3. Restart the Oracle HTTP Server, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components,"](#) to activate the configuration change.

Note: Oracle Directory Services Manager loses its connection and displays a session time-out message if the Oracle WebLogic Server in the cluster that it is connected to fails. Oracle Directory Services Manager requests is routed to the secondary Oracle WebLogic Server in the cluster that you identified in the httpd.conf file after you log back in to Oracle Directory Services Manager.

20.9.3.7 ODSM is Not Accessible

Problem

Attempting to access Oracle Directory Services Manager using a web browser fails.

Solution

- Verify the Oracle Virtual Directory server is running. The Oracle Virtual Directory server must be running to connect to it from Oracle Directory Services Manager.
- Verify you entered the correct credentials in the Server, Port, User Name and Password fields. You can execute an ldapbind command against the target Oracle Virtual Directory server to verify the server, user name, and password credentials.
- Verify you are using a supported browser. Oracle Directory Services Manager supports the following browsers:
 - Internet Explorer 7
 - Firefox 2.0.0.2 and 3.0
 - Safari 3.1.2 (desktop)
 - Google Chrome 0.2.149.30

Note: While Oracle Directory Services Manager supports all of the preceding browsers, only Internet Explorer 7 and Firefox 2.0.0.2 are certified.

20.9.4 Troubleshooting Oracle Access Manager 11g

This section describes some common problems that can arise with Oracle Access Manager and the actions you can take to resolve the problem. It contains the following topics:

- [Section 20.9.4.1, "Fusion Applications Preverify Fails to Validate OAM Admin Users"](#)
- [Section 20.9.4.2, "User Reaches the Maximum Allowed Number of Sessions"](#)
- [Section 20.9.4.3, "Policies Do Not Get Created When Oracle Access Manager is First Installed"](#)
- [Section 20.9.4.4, "You Are Not Prompted for Credentials After Accessing a Protected Resource"](#)
- [Section 20.9.4.5, "Cannot Log In to OAM Console"](#)

- [Section 20.9.4.6, "Unable to Create Keystore – Unable to Load Key"](#)
- [Section 20.9.4.7, "Error When Starting OAM Managed Servers on Windows"](#)

20.9.4.1 Fusion Applications Preverify Fails to Validate OAM Admin Users

Problem

The Fusion Applications preverify step, described in the task "Run the pre-verify phase" in *Oracle Fusion Applications Customer Relationship Management Enterprise Deployment Guide*, fails to validate OAM Admin users. In the OAM diagnostic file, you see an error similar to this:

```
Caused by: oracle.security.idm.OperationFailureException:
@ oracle.security.am.common.jndi.ldap.PoolingException [Root exception is
@ oracle.ucp.UniversalConnectionPoolException: Invalid life cycle state. Check
@ the status of the Universal Connection Pool]
```

Solution

1. Shut down the administration server and all managed servers in the domain, as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)
2. Delete the files with names of the form:
 /tmp/UCP*
3. Restart the administration server and managed servers.

20.9.4.2 User Reaches the Maximum Allowed Number of Sessions

Problem

The Oracle Access Manager server displays an error message similar to this:

```
The user has already reached the maximum allowed number of sessions. Please close
one of the existing sessions before trying to login again.
```

Solution

If users log in multiple times without logging out, they might overshoot the maximum number of configured sessions. You can modify the maximum number of configured sessions by using the OAM Administration Console.

To modify the configuration by using the OAM Administration Console, proceed as follows:

1. Go to **System Configuration -> Common Settings -> Session**
2. Increase the value in the **Maximum Number of Sessions per User** field to cover all concurrent login sessions expected for any user. The range of values for this field is from 1 to any number.

20.9.4.3 Policies Do Not Get Created When Oracle Access Manager is First Installed

Problem

The Administration Server takes a long time to start after configuring Oracle Access Manager.

Solution

Tune the OAM database. When the Administration server first starts after configuring Oracle Access Manager, it creates a number of default policies in the database. If the database is distant or in need of tuning, this can take a significant amount of time.

Resources

```
Authentication Policies
  Protected Higher Level Policy
  Protected Lower Level Policy
  Public Policy
Authorization Policies
  Authorization Policies
```

If you do not see these items, the initial population has failed. Check the Administration Server log file for details.

20.9.4.4 You Are Not Prompted for Credentials After Accessing a Protected Resource**Problem**

When you access a protected resource, Oracle Access Manager should prompt you for your user name and password. For example, after creating a simple HTML page and adding it as a resource, you should see credential entry screen.

Solution

If you do not see the credential entry screen, perform the following steps:

1. Verify that Host Aliases for IDMDomain have been set. You should have aliases for IDMDomain:80, IDMDomain:Null:, admin.mycompany.com:80, and sso.mycompany.com:443.
2. Verify that WebGate is installed.
3. Verify that OBAccessClient.xml was copied from *ASERVER_HOME/output* to the WebGate Lib directory and that OHS was restarted.
4. When OBAccessClient.xml was first created, the file was not formatted. When the OHS is restarted, reexamine the file to ensure that it is now formatted. OHS gets a new version of the file from Oracle Access Manager when it first starts.
5. Shut down the Oracle Access Manager servers and try to access the protected resource. You should see an error saying Oracle Access Manager servers are not available. If you do not see this error, re-install WebGate.

20.9.4.5 Cannot Log In to OAM Console**Problem**

You cannot log in to the OAM Console. The Administration Server diagnostic log might contain an error message similar to this:

```
Caused by: oracle.security.idm.OperationFailureException:
oracle.security.am.common.jndi.ldap.PoolingException [Root exception is
oracle.ucp.UniversalConnectionPoolException:
Invalid life cycle state.
Check the status of the Universal Connection Pool]
at
oracle.security.idm.providers.stdldap.UCPool.acquireConnection(UCPool.java:112)
```

Solution

Remove the /tmp/UCP* files and restart the Administration Server.

20.9.4.6 Unable to Create Keystore – Unable to Load Key

Problem

You are trying to set up the keystore, as described in [Section 13.10.3, "Setting up Keystore with the SSL Certificate and Private Key File of the Access Client."](#) When you try to run the create keystore command:

```
openssl pkcs8 -topk8 -nocrypt -in ASERVER_HOME/output/Webgate_IDM/aaa_key.pem
-inform PEM -out aaa_key.der -outform DER
```

you receive the error:

```
Unable to load key.
```

Solution

You have a password mismatch. To correct this, go to the OAM console, reset the WebGate Access Client password and try again.

20.9.4.7 Error When Starting OAM Managed Servers on Windows

Problem

On Windows, when you start the OAM managed servers, you see an error similar to this:

```
Caused by: java.net.SocketException: Address family not supported by protocol
family: bind
```

Solution

Edit `setDomainEnv.cmd`, which is located in `MSERVER_HOME/bin` and add the following parameters to the environment variable `EXTRA_JAVA_PROPERTIES`:

```
-DuseIPv6Address=false -Djava.net.preferIPv6Addresses=false
```

Restart the Administration Server and all Managed Servers that are running.

20.9.5 Troubleshooting Oracle Identity Manager

This section describes some common problems that can arise with Oracle Identity Manager and the actions you can take to resolve the problem. It contains the following topics:

- [Section 20.9.5.1, "java.io.FileNotFoundException When Running Oracle Identity Manager Configuration"](#)
- [Section 20.9.5.2, "ResourceConnectionValidationException When Creating User in Oracle Identity Manager"](#)

20.9.5.1 java.io.FileNotFoundException When Running Oracle Identity Manager Configuration

Problem

When you run Oracle Identity Manager configuration, the error `java.io.FileNotFoundException: soaconfigplan.xml (Permission denied)` may appear and Oracle Identity Manager configuration might fail.

Solution

To workaroud this issue:

1. Delete the file `/tmp/oaconfigplan.xml`.
2. Start the configuration again (`OH/bin/config.sh`).

20.9.5.2 ResourceConnectionValidationxception When Creating User in Oracle Identity Manager

Problem

If you are creating a user in Oracle Identity Manager (by logging into Oracle Identity Manager, clicking the Administration tab, clicking the **Create User** link, entering the required information in the fields, and clicking **Save**) in an active-active Oracle Identity Manager configuration, and the Oracle Identity Manager server that is handling the request fails, you may see a "ResourceConnectionValidationxception" in the Oracle Identity Manager log file, similar to:

```
[2010-06-14T15:14:48.738-07:00] [oim_server2] [ERROR] [] [XELLERATE.SERVER]
[tid: [ACTIVE].ExecuteThread: '0' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: xelsysadm] [ecid:
004YGJGmYrtEkJV6u3M6UH00073A0005EI,0:1] [APP: oim#11.1.1.3.0] [dcid:
12eb0f9c6e8796f4:-785b18b3:12938857792:-7ffd-0000000000000037] [URI:
/admin/faces/pages/Admin.jspx] Class/Method:
PooledResourceConnection/heartbeat encounter some problems: Operation timed
out[[
com.oracle.oim.gcp.exceptions.ResourceConnectionValidationxception: Operation
timed out
    at
oracle.iam.ldapsync.impl.repository.LDAPConnection.heartbeat(LDAPConnection.ja
va:162)
    at
com.oracle.oim.gcp.ucp.PooledResourceConnection.heartbeat(PooledResourceConnec
tion.java:52)
    .
    .
    .
```

Solution

Despite this exception, the user is created correctly.

20.9.6 Troubleshooting Oracle Identity Federation

This section describes some common problems that can arise with Oracle Identity Federation and the actions you can take to resolve the problem. It contains the following topics:

- [Section 20.9.6.1, "Cannot Log In to the Oracle Identity Federation Server \(Windows\)"](#)
- [Section 20.9.6.2, "Extending the Domain with Oracle Identity Federation Fails"](#)
- [Section 20.9.6.3, "Cannot Change Oracle Identity Federation Parameters by Using Fusion Middleware Control"](#)

20.9.6.1 Cannot Log In to the Oracle Identity Federation Server (Windows)

Problem

On a Windows system, you cannot log in to the Oracle Identity Federation server even though it is running.

Solution

Make sure that the Oracle Identity Federation server is using IPv4, if everything else is using IPv4).

To verify this, look in the file `ASERVER_HOME/bin/setDomainEnv.cmd` on `IDMHOST1` and `IDMHOST2`.

Locate the line `EXTRA_JAVA_PROPERTIES` and add the following to the entry if it is not already present:

```
-Djava.net.preferIPv6Addresses -DuseIPv6Address=false
-Djava.net.preferIPv6Addresses=false
```

Save the file and restart the Oracle Identity Federation servers as described in [Section 20.1, "Starting and Stopping Oracle Identity Management Components."](#)

20.9.6.2 Extending the Domain with Oracle Identity Federation Fails

Problem

Extending the domain with Oracle Identity Federation fails when Oracle Identity Manager is installed at the Create Managed Server step.

Solution

Copy the file `setDomainEnv.sh` from `ASERVER_HOME/bin` on `IDMHOST1` to `OIFHOST1`.

Retry the operation.

20.9.6.3 Cannot Change Oracle Identity Federation Parameters by Using Fusion Middleware Control

Problem

You cannot change Oracle Identity Federation parameters by using Oracle Enterprise Manager Fusion Middleware Control. You see the message:

```
Configuration settings are unavailable because ..... OIF .....
is down
```

even though Oracle Identity Federation is up and running.

Solution

Here are the common causes and resolutions:

1. Oracle Identity Federation is up but the EM agent is down.
 - a. Check the EM agent status by running:


```
ORACLE_INSTANCE/EMAGENT/EMAGENT/bin/emctl status agent
```
 - b. Start the EM agent, if it is down, by running:


```
ORACLE_INSTANCE/bin/opmnctl startproc ias-component=EMAGENT
```
 - c. Log in to Fusion Middleware Control again.
2. Oracle Identity Federation and EM agent are up, but the OIF home page and configuration pages in Fusion Middleware Control still show: **OIF is down**.
 - a. Check if the EM agent points to the correct Fusion Middleware Control by running:


```
ORACLE_INSTANCE/EMAGENT/EMAGENT/bin/emctl status agent
```

Verify that the host and port for property Repository URL are the same as the Fusion Middleware Control's host and port.
 - b. If the host and port are mismatched, change the Repository URL in EM agent to the correct Fusion Middleware Control by running:


```
ORACLE_INSTANCE/EMAGENT/EMAGENT/bin/emctl switchOMS  
http(s)://Host:Port/em/upload'
```
 - c. Log in to Fusion Middleware Control again.
3. If the issue still exists, once logged in to Fusion Middleware Control, navigate to **Farm->Agent-Monitored Targets** (Top Left corner of the page) and click the **Configure** icon of the row that refers to Oracle Identity Federation. On the next page, ensure that all the information is correct and complete. Click **OK** to confirm.

Check that the WebLogic user name and password are present.

Check the host value. It might have been specified with an IPv6 address format.
4. If the issue still exists, restart the EM agent.
 - a. Stop the EM agent by running:


```
INST_HOME/bin/opmnctl stopproc ias-component=EMAGENT
```
 - b. Start the EM agent by running:


```
INST_HOME/bin/opmnctl startproc ias-component=EMAGENT
```
 - c. Log in to Oracle Enterprise Manager Fusion Middleware Control again.

Index

A

- Access Manager
 - See Oracle Access Manager
- Access Server
 - defined, 13-1
- Active Directory
 - configuring for Oracle Access Manager and Oracle Identity Manager, 11-10
- adapters
 - Oracle Virtual Directory, 12-11
- administration server, 8-17
- application tier, 2-7
 - backing up the configuration, 10-8
 - scaling out, 20-21
 - scaling up, 20-11
- Audit Framework
 - introduction, 20-33
- auditing Identity Management, 20-33

B

- backup
 - after setting up Oracle HTTP Server, 6-5
 - and recovery, 20-36
 - LDAP directories, 11-1
 - of runtime artifacts, 20-37
 - of static artifacts, 20-36
 - of the application tier configuration, 10-8
 - WebLogic domain, 8-28
- backups
 - installation, 18-19
- boot.properties file
 - creating, 8-13, 8-14
 - updating on IDMHOST1 and IDMHOST2, 19-6

C

- certificate
 - generating for Identity Management Domain, 9-10
 - host name verification, 16-2
 - self-signed, 16-3
- cluster agent, 1-3
- clusters, 1-3
- clusterware, 1-3

- Coherence, see 'Oracle Coherence'
- component
 - patching, 20-38
- configuration
 - Oracle Coherence, 14-6
 - shared storage, 4-8
- Configuration Wizard
 - creating domain with, 8-4
- configuring
 - custom keystores for Node Manager, 16-6
 - database for Oracle Fusion Middleware metadata, 5-6
 - database repository, 5-1
 - firewall, 3-11
 - Node Manager, 16-1
 - Oracle Internet Directory instances Oracle Internet Directory
 - configuring instances, 9-2
 - ports for load balancer, 3-4
 - targets for server migration, 17-6
 - virtual hosts, 7-3
 - virtual server names on load balancer, 3-4
- Configuring Oracle Access Manager with Web Tier, 14-11
- creating Fusion Middleware home, 6-7
- credential store
 - reassociating with Oracle Internet Directory, 11-4
- custom keystores, 16-6

D

- data source, 17-2
- database
 - adding a service, 5-7
 - CREATE_SERVICE subprogram, 5-7
 - creating services, 5-6
 - Oracle Real Application Clusters, 5-2
 - required, 5-2
 - starting a service, 5-7
 - versions, 5-3
- directory structure
 - recommendations, 4-3
 - terminology, 4-1
- directory tier, 2-5
 - scaling out, 20-20
 - scaling up, 20-10

- disabling host name verification, 8-19
- DNS, virtual server names and, 3-2
- DOMAIN directory
 - defined, 4-2
- domain directory, 8-17

E

- enabling WebLogic plug-in, 8-23
- enterprise architecture, 2-8
- enterprise deployment
 - hardware requirements, 2-10
 - high availability, 1-6
 - patching, 20-37
 - port assignment, 3-11
 - ports used, 3-11
 - scaling, 20-10
 - scaling out, 20-20
 - scaling up, 20-10
 - security, 1-5
- enterprise topologies, 2-1
- environment privileges, 17-5
- etc/services file, 10-2

F

- failback, 1-2
- failover, 1-2
- file
 - etc/services, 10-2
- firewall
 - configuring, 3-11
- Fusion Middleware components
 - installing, 6-5
- Fusion Middleware home
 - installing, 6-6

G

- generating self-signed certificates, 16-3
- grid servers, 1-1

H

- hardware cluster, 1-3
- high availability, 2-9, 14-6
- high availability practices, Oracle site, 1-2
- host name
 - network, 1-4
 - physical, 1-4
 - virtual, 1-4
- host name verification
 - certificate for Node Manager, 16-2
 - disabling, 8-19
 - managed servers, 16-8
- HTTP server
 - configuring for WebLogic Administration Server, 8-20, 8-21
 - installing, 6-3
 - registering with WebLogic Server, 8-22

I

- identity keystore, 16-4
- Identity Management components
 - stopping and starting, 20-1
- identity store
 - preparing, 11-6
 - usage, 9-1
- idmhost-vip.mycompany.com
 - virtual IP address for WebLogic Administration Server, 3-8
- installation
 - Fusion Middleware home, 6-7
 - Oracle WebLogic Server, 6-7
- installing
 - Fusion Middleware components, 6-5
 - Fusion Middleware home, 6-6
 - HTTP server, 6-3
 - Oracle Fusion Middleware, 6-5
 - Oracle HTTP Server, 6-3
 - Oracle Identity and Access Management, 6-11
 - Oracle Identity Management, 6-8
 - software, 6-1
- IPs, 3-10

K

- keystores
 - custom, 16-6
 - identity, 16-4
 - trust, 16-5
- Keytool utility, 16-5

L

- LDAP configuration post-setup script, 14-10
- LDAP directories
 - backing up, 11-1
- leasing table for server migration, 17-1
- leasing.ddl script, 17-2
- load balancer
 - configuring ports, 3-4
 - configuring virtual server names, 3-4
 - required features, 3-5
- log file for Node Manager, 16-2

M

- managed servers, 8-17
 - custom keystores, 16-6
 - host name verification, 16-8
 - provisioning, 10-5
- mapping of IPs and VIPs, 3-10
- Middleware home, 1-2
- monitoring
 - Oracle Internet Directory, 20-8
 - Oracle Virtual Directory, 20-9
- multi data source, 17-2
- MW_HOME
 - defined, 4-2

N

- network host name, 1-4
- Node Manager, 16-3
 - custom keystores, 16-6
 - described, 16-1
 - host name verification certificate, 16-2
 - identity keystore, 16-4
 - log file, 16-2
 - properties file, 17-4
 - setup, 16-1
 - trust keystore, 16-5
- Node Manager properties file, 16-2
- nodes
 - primary, 1-3
 - secondary, 1-3
- non-OID directories
 - creating access control lists, 11-12

O

- ODSM
 - see Oracle Directory Services manager
- Oracle Access Manager
 - and Oracle Identity Manager topology, 2-2
 - configuring with Web Tier, 13-3
 - creating identity asserter, 19-4
 - defined, 13-1
 - extending directory schema, 11-8
 - Oracle Access Protocol (OAP), 3-14
 - Oracle Identity Protocol (OIP), 3-14
 - overview of user access requests, 3-14
 - testing server migration, 17-7
 - troubleshooting, 20-45
- Oracle Access Manager 11g, 13-1
 - integrating with Oracle Identity Manager, 18-1
- Oracle Access Protocol (OAP), 3-14
- Oracle BI EE
 - upgrade roadmap table, 2-14
- Oracle Coherence, 14-6
- Oracle Directory Integration Platform
 - configuring the first instance, 10-2
 - configuring the second instance, 10-3
 - installing the first instance, 10-2
 - installing the second instance, 10-3
- Oracle Directory Services Manager
 - configuring the first instance, 10-2
 - configuring the second instance, 10-3
 - console and OHS, 10-7
 - creating connections to Oracle Virtual Directory, 12-11
 - installing the first instance, 10-2
 - installing the second instance, 10-3
 - scaling out, 20-22
 - scaling up, 20-12
 - troubleshooting, 20-42
 - validating, 10-7
- Oracle Directory Services Manager and Oracle Web Tier, 10-6
- Oracle Enterprise Manager
 - monitoring Oracle Internet Directory, 20-8
 - monitoring Oracle Virtual Directory, 20-9
- Oracle Fusion Middleware
 - enterprise deployment functions, 1-1
 - installing, 6-5
- Oracle Fusion Middleware (FMW)
 - creating FMW home, 6-7
 - installing Oracle WebLogic Server, 6-7
- Oracle home, 1-2
- Oracle HTTP Server
 - installing, 6-3
- Oracle HTTP Server (OHS)
 - backing up, 6-5
- Oracle Identity and Access Management
 - installing, 6-11
- Oracle Identity Federation
 - configuring, 15-2
 - described, 15-1
 - topology, 2-4
 - troubleshooting, 20-49
- Oracle Identity Management
 - installing, 6-8
- Oracle Identity Manager
 - creating a multi data source, 17-3
 - defined, 14-2
 - integrating with Oracle Access Manager 11g, 18-1
 - troubleshooting, 20-48
 - verifying server migration, 17-8
- Oracle Identity Protocol (OIP), 3-14
- Oracle instance, 1-2
- Oracle Internet Directory
 - backing up, 9-16
 - component names assigned by installer, 20-8
 - monitoring, 20-8
 - scaling out, 20-21
 - scaling up, 20-10
 - troubleshooting, 20-39
- Oracle Real Application Clusters database, 5-2
- Oracle Virtual Directory
 - backing up, 12-15
 - configuring SSL Server Authentication Mode, 12-7
 - creating adapters, 12-11
 - creating Oracle Directory Services Manager connections to, 12-11
 - monitoring, 20-9
 - scaling out, 20-21
 - scaling up, 20-11
 - troubleshooting, 20-40
- Oracle WebLogic Administration Server
 - See WebLogic Administration Server
- Oracle WebLogic Server (WLS)
 - installation, 6-7
- Oracle WebLogic Server Clusters
 - See WebLogic Server Clusters
- Oracle WebLogic Server domain
 - See WebLogic Server domain
- Oracle WebLogic Server home
 - See WebLogic Server home
- ORACLE_BASE
 - defined, 4-1

ORACLE_HOME
 defined, 4-2
ORACLE_INSTANCE
 defined, 4-2

P

patching
 of a component, 20-38
 of a source file, 20-37
 of an enterprise deployment, 20-37
performance, enterprise deployment and, 1-1
persistence store, 14-16
physical host name, 1-4
physical IP, 1-4
Policy Store
 preparing, 11-2
policy store
 reassociating with Oracle Internet Directory, 11-4
port
 freeing, 10-2
port assignment, 3-11
ports
 configuring for load balancer, 3-4
 used in enterprise deployment, 3-11
primary node, 1-3
properties file of Node Manager, 17-4
provisioning managed servers, 10-5

R

RCU
 creating Identity Management schemas, 5-9
reference topology, 2-1
registering Oracle Internet Directory with WebLogic
 Server domain, 9-8
registering Oracle Virtual Directory with WebLogic
 Server domain, 12-6

S

scaling
 of enterprise deployments, 20-10
scaling out
 application tier, 20-21
 directory tier, 20-20
 enterprise deployment, 20-20
 Oracle Directory Services Manager, 20-22
 Oracle Internet Directory, 20-21
 Oracle Virtual Directory, 20-21
 web tier, 20-33
scaling up
 application tier, 20-11
 directory tier, 20-10
 enterprise deployment, 20-10
 Oracle Directory Services Manager, 20-12
 Oracle Internet Directory, 20-10
 Oracle Virtual Directory, 20-11
 web tier, 20-20
scripts
 leasing.ddl, 17-2

 wlsifconfig.sh, 17-5
secondary node, 1-3
security, 2-9
self-signed certificate, 16-3
server migration
 configuring targets, 17-6
 creating a multi data source, 17-2
 editing Node Manager's properties file, 17-4
 leasing table, 17-1
 multi data source, 17-2
 setting environment and superuser
 privileges, 17-5
 setting up user and tablespace, 17-1
 testing, 17-7
service
 assigning to an instance, 5-7
service level agreements, 1-1
setting up Node Manager, 16-1
shared storage, 1-3
 configuration, 4-8
Single Sign-On
 validating for Oracle Access Manager, 19-10
Single Sign-on
 configuring for administration consoles, 19-1
SOAHOST
 creating Fusion Middleware home, 6-7
 installing Oracle WebLogic Server, 6-7
SOAHOST1VHn virtual hosts, 14-6
software
 Oracle WebLogic Server, 6-7
software installation, 6-1
 summary, 6-2
source file
 patching, 20-37
SSL
 configuring ports for LDAP and Oracle Internet
 Directory, 3-2
 server authentication mode, 9-12, 12-7
starting
 Identity Management components, 20-1
stopping
 Identity Management components, 20-1
superuser privileges, 17-5
switchback, 1-4
switchover, 1-4

T

tablespace for server migration, 17-1
TAF settings, 5-7
targets for server migration, 17-6
terminology
 directory structure, 4-1
 DOMAIN directory, 4-2
 MW_HOME, 4-2
 ORACLE_BASE, 4-1
 ORACLE_HOME, 4-2
 ORACLE_INSTANCE, 4-2
 WL_HOME, 4-2
testing of server migration, 17-7

- timeouts for SQL*Net connections
 - preventing, 20-39
- topology
 - enterprise, 2-1
 - reference, 2-1
- Transparent Application Failover settings, 5-7
- troubleshooting
 - Oracle Access Manager, 20-45
 - Oracle Directory Services Manager, 20-42
 - Oracle Identity Federation, 20-49
 - Oracle Identity Manager, 20-48
 - Oracle Internet Directory, 20-39
 - Oracle Virtual Directory, 20-40
- trust keystore, 16-5

U

- unicast communication, 14-6
- utils.CertGen utility, 16-3
- utils.ImportPrivateKey utility, 16-4

V

- validating
 - Oracle Access Manager Single Sign-On, 19-10
- validation
 - server migration, 17-7
- VIPs, 3-10
- virtual host name, 1-4
- virtual hosts, 7-3
- virtual IP, 1-4
- virtual IP address, 3-8
 - associating weblogic Administration Server, 8-3
 - configuring for WebLogic Administration Server, 3-8
- virtual IPs (VIPs), 3-10

W

- web tier, 2-9
 - scaling out, 20-33
 - scaling up, 20-20
- WebGate
 - configuring, 19-7
 - defined, 13-1
 - installing, 19-7
- WebLogic
 - backing up domain, 8-28
 - enabling plug-in, 8-23
- WebLogic Administration Server
 - associating with virtual IP address, 8-3
 - configuring virtual IP address for, 3-8
 - failing over, 8-24
 - front end URL, 8-23
- WebLogic Server domain
 - considerations, 3-15
 - registering Oracle Internet Directory, 9-8
 - registering Oracle Virtual Directory, 12-6
- WebLogic Server home, 1-2
- WL_HOME
 - defined, 4-2

